

Exhibit C

17 MAG 6961

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of an Application for
Search Warrants for Stored Electronic
Communications

**SEALED
AGENT AFFIDAVIT**

____ Mag. _____

**Application for Search Warrants
for Stored Electronic Communications**

STATE OF NEW YORK)
) ss.
COUNTY OF NEW YORK)

JEFF D. DONALDSON, being duly sworn, deposes and states:

I. Introduction

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI") assigned to the New York Field Office, and have been employed by the FBI since 2010. I am currently assigned to a squad responsible for counterespionage matters and have worked in the field of counterintelligence from 2010 to present. In the course of my duties as a Special Agent, I am responsible for investigating offenses involving espionage and related violations of law, including unauthorized retention, gathering, transmitting or losing classified documents or materials; unauthorized removal and retention of classified documents or materials; illegally acting in the United States as a foreign agent; other national security offenses; and the making of false statements. As a result of my involvement in espionage investigations and investigations involving the unauthorized disclosure or retention of classified information, as well as my training in counterintelligence operations, I am familiar with the tactics, methods, and techniques of United States persons who possess, or have possessed a United States Government security clearance and may choose to harm the United States by misusing their access to classified

information. I am also familiar, though my training and experience with the use of computers in criminal activity and the forensic analysis of electronically stored information.

2. **Basis for Knowledge.** This Affidavit is based upon my participation in the investigation, my examination of reports and records, and my conversations with other law enforcement agents and other individuals, as well as my training and experience. Because this Affidavit is being submitted for the limited purpose of obtaining the Requested Information, it does not include all the facts that I have learned during the course of this investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated. In addition, unless otherwise indicated, statements by others referenced in this Affidavit were not necessarily made to me, but may have been provided to me by someone else to whom I have spoken or whose report I have read (and who in turn may have had either direct or indirect knowledge of the statement). Similarly, unless otherwise indicated, information in this Affidavit resulting from surveillance does not necessarily set forth my personal observations, but may have been provided to me by other law enforcement agents who observed the events, and to whom I have spoken or whose report I have read.

II. The Target Accounts

3. I make this affidavit in support of an application for search warrants pursuant to 18 U.S.C. § 2703 directed to Google, Inc., headquartered in Mountain View, CA (“Google”); Reddit, Inc., headquartered in San Francisco, CA (“Reddit”), and Github.com, headquartered in Sacramento, CA (“GitHub”), (collectively, “Providers”), for all content and other information associated with the following “**Target Accounts**”:

a. The Google account associated with the email address joshschulte1@gmail.com (the “**Subject Google Account**”), which is maintained and controlled by Google.

b. The Reddit account associated with the account name L1347517 (the “**Subject Reddit Account**”), which is maintained and controlled by Reddit.

c. The GitHub account associated with the user name pedbsktbll (the “**Subject GitHub Account**”), which is maintained and controlled by GitHub.

4. The information to be searched is described in the following paragraphs and in Attachment A to each of the proposed warrants.

Google

5. Based on my training, experience, and participation in this investigation, I know the following about Google:

a. Google offers email and other Internet-based services to the public. Among other things, Google allows subscribers to maintain email accounts under the domain name gmail.com. A subscriber using Google’s services can access his or her email account from any computer connected to the Internet, and can link any variety of Google’s other Internet-based services to his/her Gmail account.

b. Google maintains the following records and information with respect to every subscriber account:

i. *Email contents.* In general, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber’s account, or stored in draft form in the account, is maintained on Google’s servers unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on Google’s computers

indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

ii. *Address book.* Google also allows subscribers to maintain the equivalent of an address book, comprising email addresses and other contact information of other email users.

iii. *Subscriber and billing information.* Google collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. Google also maintains records concerning the date on which the account was created, the Internet protocol ("IP") address of the user at the time of account creation, the current status of the account (*e.g.*, active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying subscribers, Google maintains records of the subscriber's means and source of payment, including any credit card or bank account number.

iv. *Transactional information.* Google also typically retains certain transactional information about the use of each account on its system. This information can include records of login (*i.e.*, session) times and durations and the methods used to connect to the account (such as logging into the account through Google's website).

v. *Customer correspondence.* Google also typically maintains records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber's account.

vi. *Preserved records.* Google also maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f).

c. In addition, subscriber information for the Subject Google Account indicates that the subscriber of the Subject Google Account has activated additional online Google Services, and, accordingly, the Provider also maintains, among other things, the following records and information with respect to the **Subject Google Account**:

i. *Google Drive*. Google provides users with a certain amount of free “cloud” storage, currently 15 gigabytes, through the service called “Google Drive” (users can purchase a storage plan through Google to store additional content). Users can use their Google Drive to store email, attachments, videos, photographs, documents, and other content “in the cloud,” that is online. A user can access content stored on Google Drive by logging into his or her Google account through any computer or other electronic device that is connected to the Internet. Users can also share files stored on Google Drive with others, allowing them to view, comment, and/or edit the files.

ii. *Google Docs*. Google provides users with the ability to write, edit, and collaborate on various documents with other Google users through a service called “Google Docs.” Users can use Google Docs to create online documents that can be stored on or saved to the user’s Google Drive. Users can also download such documents in various formats, such as a Microsoft Word document (e.g., “.docx”), an OpenDocument Format (“.odt”), Rich Text Format (“.rtf”), a PDF document (“.pdf”), or Plain Text document (“.txt”).

iii. *Google Photos*. Google provides users with a certain amount of free storage for photographs, through a service called Google Photos, which allows users to manually store photographs and videos, and which automatically uploads photographs and videos taken by registered mobile devices. Google also retains the metadata—or data that provides information about the data in question, such as the time and date of creation, the author or creator, the means

of its creation, the purpose of the data, among other data—for photos and videos that are uploaded to Google, including to Google Photos. This metadata includes what is known as exchangeable image file format (or “Exif”) data, and can include GPS location information for where a photo or video was taken.

iv. *Google Calendar*. Google provides users with an online calendar, in which they can add appointments, events, and reminders, which are synchronized across registered computers and mobile devices. Users can share their calendars with other users, allowing the maintenance of joint calendars.

v. *YouTube content*. Google allows subscribers to maintain linked YouTube accounts, a global video-sharing website that allows users to upload and share videos with public on the Internet. Registered users can upload an unlimited number of videos and add comments to videos.

vi. *Google Chats and Google Hangouts content*. Google allows subscribers to engage in “chat” sessions in an instant messaging format with other Google users, the transcripts of which are generally stored in a user’s email content. Similarly, Google allows users to engage in enhanced chat sessions, called Hangouts, which permit the sharing of additional content such as videos, sounds, and images. In general, Hangouts content is stored separately from a user’s email and chat content.

vii. *Location History data*. Google maintains recent location data, collected periodically, from mobile devices that are logged into or have used applications (or “apps”) or services provided by Google. For example, Google collects information collected from GPS, Wi-Fi networks, cell site locations, and mobile networks to estimate a user’s location.

Google apps and services also allow for location reporting, which allows Google to periodically store and use a device's most recent location data in connection with a Google account.

viii. *Android Services.* Google also maintains information relating to Android, as it relates to an account. Android is a mobile operating system that is developed by Google, and is used on a variety of touchscreen mobile devices, such as smartphones and tablet computers. Google retains information related to the Android device associated with an account, including the IMEI (the International Mobile Station Equipment Identifier), MEID (the Mobile Equipment Identifier), device ID, and/or serial number of the devices. Each of those identifiers uniquely identifies the device used. One device may be associated with multiple different Google and Android accounts, and one Google or Android account may be associated with multiple devices.

ix. *Google Voice.* Google provides a telephone service that provides call forwarding and voicemail services, voice and text messaging.

x. *Google Payments.* Google allows for the storage of payment information associated with a Google Account, including credit cards and bank accounts, and contains information about all transactions made with a Google account, allowing for the payment for goods (such as those purchased through Google Shopping) and bills, among other features.

xi. *Web History.* Google maintains searches and account browsing activity, from Chrome, Google's proprietary web browser, as well as other Google applications.

Reddit

6. Based on my training, experience, and participation in this investigation, I know the following about Reddit:

a. Reddit operates several products and services, including reddit.com, redditgifts.com, and associated Reddit mobile applications. The most popular product is reddit.com, which provides an online forum where people can create communities (known as “subreddits”) in which users can communicate online.

b. Each subreddit on reddit.com has its own page, subject matter, users, and moderators. Users post stories, links, and media to these communities, and other users can comment and can “upvote” or “downvote” a post.

c. The information that is collected by Reddit varies depending on what services the user utilizes. For example, if the user signs up to post on the website reddit.com, Reddit users can choose to provide their name and other contact information (including, but not limited to, their email address), although though users can also choose not to do so. If the user signs up to Reddit Gifts, the user may be asked to provide Reddit with personal information such name, address, telephone number, age, personal interests, and email address. The user may also be required to provide log-in information for an existing Reddit Account or to create one before using Reddit Gifts.

GitHub

7. Based on my training, experience, and participation in this investigation, I know the following about GitHub:

8. Based on my training, experience, and participation in this investigation, I know the following about GitHub:

a. GitHub is a web-based Git, or version control repository, and Internet-hosting service, that can be accessed at <https://github.com/>. GitHub allows Internet users to host code, manage projects, and build software alongside millions of other developers.

b. A user must create an account in order to contribute content to the site, but public repositories can be browsed and downloaded by others. When an individual registers for an account, they are able to discuss, manage, create repositories, submit contributions to others' repositories, and/or review changes to code. Users are represented in GitHub's system as personal GitHub accounts. Each user has a personal profile, and can own multiple repositories. Users can create or be invited to join organizations, or to collaborate on another user's repository. A repository is one of the most basic GitHub elements. It can contain project files (including documentation), and stores each file's revision history.

c. A variety of information is available on GitHub about users and their repositories. Public user profiles can include username, repositories that the user has starred, other GitHub users the user follows, and those that follow the user. A user may also choose to not share his or her real name, avatar, affiliated company, location, public email address, personal web page, or organizations to which the user belongs.

d. GitHub provides social networking-like functions such as feeds, followers, wikis (using wiki software called Gollum) and a social network graph to display how developers work on their versions of a repository and what version is newest.

e. GitHub can be accessed on GitHub.com, or through GitHub Enterprise on one's own server, or in a private cloud using Amazon Web Services. GitHub Enterprise is similar to GitHub's public service, but is designed for use by large-scale enterprise software development teams where the enterprise wishes to host their repositories behind a corporate firewall.

III. Jurisdiction to Issue the Requested Warrants

9. Pursuant to Title 18, United States Code, Sections 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as Google, Reddit, or GitHub, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

10. A search warrant under Section 2703 may be issued by “any district court of the United States (including a magistrate judge of such a court)” that “has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

11. When the Government obtains records under Section 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A) & (3). Additionally, the Government may obtain an order precluding the Provider from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

IV. The Subject Offenses

12. For the reasons detailed below, I believe that there is probable cause to believe that the Target Accounts contain evidence, fruits, and instrumentalities of (i) the unauthorized possession and, *inter alia*, the communication of national defense information to someone not entitled to receive it, in violation of Title 18, United States Code, Section 793(d); (ii) the unlawful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); (iii) exceeding authorized access to a computer in order to obtain national defense information with reason to believe that information could be used to the injury of the

United States and the advantage of a foreign nation and willfully transmitting that information to a person not entitled to receive it, in violation of Title 18, United States Code, Section 1030(a)(1); and (iv) intentionally exceeding authorized access to a computer and thereby obtaining information from a department or agency of the United States, in violation of Title 18, United States Code, Section 1030(a)(2)(B) (collectively the “Subject Offenses”).

V. Probable Cause

A. WikiLeaks Publication of Classified CIA Information

13. Based on my review of publicly available material on the Internet, including on the website wikileaks.org (“WikiLeaks”), I know that, on March 7, 2017, WikiLeaks published what it claimed were more than 8,000 documents and files that contained classified information (the “Classified Information”) belonging to the Central Intelligence Agency (“CIA”). In its press release accompanying the Classified Information, WikiLeaks further claimed that:

- a. The public dissemination of the Classified Information was “the largest ever” unauthorized publication of classified CIA documents.
- b. The Classified Information constituted the “first full part” of a series—thus indicating that there would be subsequent publications of additional sensitive CIA information.
- c. The “collection” obtained by WikiLeaks amounted to “more than several hundred million lines of code” and revealed the “entire hacking capacity” of the CIA, including various malware, viruses, and other tools used by the CIA.

14. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that:

- a. The information that WikiLeaks claimed was classified CIA information—that is, the Classified Information—was at the time of its disclosure, in fact,

classified CIA information.

b. Specifically, the Classified Information was created and maintained by one specific group within the CIA which is responsible for various computer engineering activities, including the development of computer code (the “CIA Group”). That CIA Group exists within a larger CIA component (the “CIA Component”). In March 2016, less than 200 employees were assigned to the CIA Group. And only employees of the CIA Group had access to the computer network on which the Classified Information that was stolen from the CIA Group’s computer network was stored. (Moreover, as described in detail below, only three of those approximately 200 people who worked for the CIA Group had access to the specific portion of the Group’s computer network on which the Classified Information was likely stored.)

c. The Classified Information appears to have been stolen from the CIA Component sometime between the night of March 7, 2016 and the night of March 8, 2016.

i. This is based on preliminary analysis of the timestamps associated with the Classified Information which indicates that March 7, 2016 was the latest (or most recent) creation or modification date associated with the Classified Information.

ii. Because, for the reasons described below (*see infra*), the Classified Information was apparently copied from an automated daily back-up file, it is likely that the Classified Information was copied either late on March 7, 2016 (after the March 7 nightly back-up was completed) or on March 8, 2016 (before the March 8 nightly back-up was completed).

iii. This is so because if the Classified Information was copied before the March 7 back-up, one would *not* expect to see in the Classified Information documents dated as late as March 7. And if the Classified Information was copied after the March 8 back-up, one *would* expect to see documents dated on or after March 8 because the “back-ups” occur

approximately each day.¹

d. The Classified Information was publicly released by WikiLeaks exactly one year to the day (March 7, 2017) from the latest date associated with the Classified Information (March 7, 2016).

e. The duplication and removal from the CIA Group's computer network of the Classified Information and its subsequent public dissemination via WikiLeaks was not authorized by the United States government.

f. The unauthorized disclosure of the Classified Information could—at a minimum—reasonably be expected to cause serious damage to the national security of the United States. *See* Executive Order 13526; 18 C.F.R. § 3a.11(a)(2).

g. The Classified Information is national defense information and its disclosure could reasonably be expected to be used to the injury to the United States and to the advantage of a foreign nation. *See* 18 U.S.C. § 793(d) & (e).

B. The CIA Group's Local Area Computer Network (LAN) and Back-Up Server

15. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that the Classified Information originated

¹ It is of course possible that the Classified Information was copied later than March 8, 2016 even though the creation/modification dates associated with it appear to end on March 7, 2016. For example, the individual who copied and removed the data could have limited his or her copying to data that was modified or created on or before March 7, 2016. (Conversely, however, the Classified Information is unlikely to have been copied before March 7, 2016, because it contains data that was created as recently as March 7, 2016.) Because the most recent timestamp on the Classified Information reflects a date of March 7, 2016, preliminary analysis indicates that the Classified Information was likely copied between the end of the day on March 7 and the end of the day on March 8.

in a specific isolated local area computer network (“LAN”) used exclusively by the CIA Group.² As described above, in and around March 2016, in total less than 200 people had access to the CIA Group’s LAN on which the Classified Information was stored.

a. An isolated network, such as the CIA Group’s LAN, is a network-security structure by which the isolated network is physically separated (or “air-gapped”) from unsecured networks, such as the public Internet.

b. Accordingly, such isolated networks, like the LAN, cannot be accessed from the public Internet, but rather only through those computers which are physically connected to the isolated network.

c. The CIA Group’s LAN, and each of its component parts, was maintained in heavily physically secured governmental facilities, which include multiple access controls and various other security measures.

d. The isolated LAN used by the CIA Group was comprised of multiple networked computers and servers. (Each of these component computers and servers were, by definition, inside the electronically isolated LAN.)

i. In order to preserve and protect the CIA Group employees’ day-to-day computer engineering work, that work was backed up, on an approximately daily basis, to another server on the CIA Group’s LAN that was used to store back-up data (the “Back-Up Server”).

ii. Back-ups of the sort stored on the Back-Up Server are designed to ensure that, should the original data be corrupted or deleted, the stored data is not lost, but rather—because of the daily back-ups—is maintained via the daily copies stored on the Back-Up

² In its press release announcing the publication of the Classified Information, WikiLeaks stated that the Classified Information originated from “an isolated, high-security network.”

Server.

C. The Publicly Disclosed Classified Information Likely Originated on the CIA Group's Back-Up Server

16. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I understand that the Classified Information that was publicly released by WikiLeaks appears likely to have been copied—specifically—from the CIA Group's Back-Up Server.

a. As described above, the Back-Up Server served as a secondary storage location for data that principally resided on the primary computer network used for CIA Group employees' day-to-day work writing computer code. Approximately each day, an automated process would back-up that data to the Back-Up Server. Each of those daily back-ups was akin to an electronic "snapshot" of the data on that particular date. In that way, the Back-Up Server simultaneously acquired and stored, on a rolling basis, daily snapshots of the original data.

b. As such, if the data contained on the Back-Up Server was copied *en masse* directly from that Server, the copy would contain numerous iterations (or snapshots) of the similar or same data which had been backed up from the original data, distinguished by date.

c. The publicly released Classified Information does in fact contain numerous iterations (or snapshots) of the similar or same data, distinguished by date.

d. Accordingly, the fact that the Classified Information contains numerous iterations (or snapshots) of the similar or same data, distinguished by date, is strongly supportive of the fact that the Classified Information was taken from the CIA Group's Back-Up Server.³

³ I understand, based on my conversations with others familiar with the CIA Group's LAN that it would be difficult, if not impossible, to copy from the data (not on the Back-Up Server) the multiple different date-distinguished iterations of the same data that are included in the publicly released Classified Information. In contrast, a single copy of the Back-Up Server

e. As described above, because the most recent timestamp associated with the Classified Information appears to be March 7, 2016, it is likely that the Classified Information was copied from the Back-Up Server after the daily back-up on March 7, 2016, and before the daily back-up on March 8, 2016.

D. TARGET SUBJECT JOSHUA ADAM SCHULTE Was One of Only Three Employees Across the Entire CIA Who, in March 2016, Had Been Given System Administrator Access to the Back-Up Server

17. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that the CIA Group's LAN was designed such that only those employees who were specifically given a particular type of systems-administrator access ("Systems Administrators") could access the Back-Up Server.

a. Systems Administrators were given a particular username and password in order to log on to and access the Back-Up Server.

b. Conversely, CIA employees who were not designated Systems Administrators were not given access to the Back-Up Server.⁴

18. I know, based on my conversations with other law enforcement agents and others, in approximately March 2016—the month when the Classified Information is assessed to have been copied—only three CIA employees were designated Systems Administrators with access to the CIA Group's Back-Up Server.

would likely include each of the prior iterations (or snapshots) of the same data—which is exactly what is reflected in the publicly released Classified Information.

⁴ It is, of course, possible that an employee who was not a designated Systems Administrator could find a way to gain access to the Back-Up Server. For example, such an employee could steal and use—without legitimate authorization—the username and password of a designated Systems Administrator. Or an employee lacking Systems Administrator access could, at least theoretically, gain access to the Back-Up Server by finding a "back-door" into the Back-Up Server.

a. TARGET SUBJECT JOSHUA ADAM SCHULTE (“SCHULTE”) was one of those three Systems Administrators.

i. SCHULTE was employed as a computer engineer by the CIA—specifically in the CIA Group—from in or about May 2010 through on or about November 10, 2016, when he resigned from the CIA.

ii. During SCHULTE’s more than six years working in the CIA Group, his responsibilities included, among other things, developing computer code for specific projects, including projects explicitly described in the Classified Information.

iii. SCHULTE had a skill set that enabled him to write computer code designed to clandestinely copy data from computers.

b. As described above, in March 2016, SCHULTE was one of only three CIA employees throughout the entire CIA who had authorized access to the CIA Group’s Back-Up Server from which the Classified Information was likely copied. The publicly released Classified Information published by WikiLeaks, based on a preliminary review, appears to contain the names and/or pseudonyms of, *inter alia*, multiple CIA employees—including two of the three aforementioned individuals with designated Systems Administrator privileges.

i. Names used by the other two CIA Group Systems Administrators were, in fact, published in the publicly released Classified Information.

ii. SCHULTE’s name, on the other hand, was not apparently published in the Classified Information.

iii. Thus, SCHULTE was the only one of the three Systems Administrators with access to the Classified Information on the Back-Up Server who was not publicly identified via WikiLeaks’s publication of the Classified Information.

c. The other two individuals who served in March 2016 as Systems Administrators for the CIA Group's LAN remain employed by the CIA. SCHULTE resigned from the CIA in November 2016, as described in detail below.

E. SCHULTE Had Access to the Back-Up Server on March 7 and 8, 2016—The Likely Dates of the Copying of the Classified Information

19. As described above, it appears likely that the Classified Information was copied between March 7 and March 8, 2016.

a. Based on my conversations with other law enforcement agents and others, and my review of documents, including access records of the CIA Component facility in which SCHULTE worked, I know that he was present at work from approximately:

- i. 10:01 a.m. until 7:16 p.m. on March 7, 2016; and
- ii. 10:19 a.m. until 7:40 p.m. on March 8, 2016.

b. Based on my conversations with other law enforcement agents and others, and my review of documents, I know that on March 8, 2016, the CIA Group held an offsite management retreat for many of its senior and midlevel managers. Accordingly, on March 8th, much of the CIA Group's management, including some to whom SCHULTE reported, were not present in the CIA Component building where SCHULTE and other CIA Group employees worked.

c. I further understand that SCHULTE's workspace (*i.e.*, his desk and computer workstation) was set up such that only three other CIA Group Employees had direct line-of-sight to SCHULTE's desk and computer—that is, only three other employees could see what he was doing at his desk. At least two of those three employees were at the offsite management retreat on March 8, 2016.

d. As described above, in March 2016, only two CIA employees in addition

to SCHULTE were designated Systems Administrators with access to the CIA Group's Back-Up Server from which the Classified Information was likely copied. On March 8, 2016, one of those two other designated Systems Administrators was at the offsite management retreat. (The retreat was held at a location that did not have any access to the CIA Group's LAN, including the Back-up Server, and therefore afforded no access to the Classified Information.)⁵

F. SCHULTE's Unauthorized Unilateral Reinstatement of His Own Administrative Privileges

20. Based on my conversations with other law enforcement agents and others, and my review of documents, I understand that, on or about April 4, 2016, around the time of his reassignment to another branch within the CIA Group, many of SCHULTE's administrator privileges on the LAN were revoked, and he was no longer permitted to serve as a Systems Administrator in the CIA Group's LAN.

a. At the same time, on or about April 4, 2016, SCHULTE's computer access to a specific developmental project ("Project-1") was also revoked. Until his reassignment, SCHULTE had been the CIA Group employee with principal responsibility for Project-1.

b. Upon that transfer, principal responsibility for Project-1 was transferred to another CIA Group employee, who received computer access to Project-1.⁶

c. I know from my review of publicly available material on the Internet, including WikiLeaks.org, that Project-1 was one of a small group of CIA projects and

⁵ On March 7 and 8, 2016, the third of the three CIA employees with Systems Administrator access was located at a CIA facility that did, in fact, have access to the Back-Up Server from which the Classified Information was likely copied.

⁶ SCHULTE retained read-only access to Project-1 (but not the ability to alter the code) and the ability to copy the computer code associated with it in order to support another project for which he had responsibility.

capabilities that WikiLeaks highlighted explicitly by name in its March 7, 2017 press release that accompanied the online publication of the Classified Information.

21. Based on my conversations with other law enforcement agents and others, and my review of documents, I understand that, less than two weeks later, on or about April 11, 2016, SCHULTE unilaterally, and without authorization, logged onto the CIA Group's LAN and reinstated his own administrator privileges.

a. On or about April 14, 2016, CIA Group management discovered that SCHULTE had personally re-instituted his administrator privileges without permission.

b. On or about April 18, 2016, SCHULTE received notice regarding CIA policies against personnel restoring their own access to privileges or computer networks after those accesses have been revoked. SCHULTE signed an acknowledgment that he understood that "individuals are not permitted to personally attempt and/or renew their previous authorizations [including administrator privileges] to any particular [computer] system." That notice further instructed SCHULTE: "do not attempt to restore or provide yourself administrative rights to any project and/or system for which they have been removed."

c. A little more than one month later, on May 26, 2016, and notwithstanding the warnings described above, SCHULTE made an official request that he again be given full access to Project-1. Before receiving a response to that request, SCHULTE requested access from another employee who, apparently without proper vetting, granted SCHULTE the requested full access to Project-1.

i. On the same day, SCHULTE used that newly obtained access to, unilaterally and without authorization, revoke the computer access permissions of all other CIA Group employees to work on Project-1.

ii. Once this conduct was discovered, SCHULTE was issued a letter of warning that stated, “You were aware of the policy for access and your management’s lack of support for you to retain administrative privileges, but nonetheless you took steps to deliberately violate that policy and gain those privileges.” It continued by warning SCHULTE that any future violations would result in “further administrative action of a more severe nature.”

iii. After receiving the letter of warning, SCHULTE disagreed with some of its conclusions and consequently refused to sign the form.

22. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that SCHULTE’s accessing of information on the LAN that he had been expressly forbidden by the CIA to access, and his accessing of information which he had been electronically prevented from accessing by the CIA, using a computer network on which he was permitted to access other, distinct information, exceeded his authorized access to the government-owned and controlled computer networks of the CIA. *See* 18 U.S.C. § 1030(a)(1) & (a)(2)(B).

G. Internal CIA Investigation of SCHULTE and a CIA Colleague

23. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that, in or around March 2016, SCHULTE came to the attention of CIA security after SCHULTE alleged that another CIA Group co-worker had made a threat against him. SCHULTE expressed deep unhappiness about the way that CIA responded to the alleged threat. He threatened legal action against the CIA for its handling of the situation, and repeatedly stated that he felt that he was being punished by CIA management for reporting the alleged threat incident. SCHULTE informed CIA security that, if “forced into a corner” he would proceed with a lawsuit against the CIA. He also repeatedly threatened that he or his lawyer would go to the media. In addition, CIA security learned that

SCHULTE had removed an internal CIA document from CIA facilities that regarded his complaints to the CIA concerning its handling of the alleged threat, despite being told multiple times by CIA security officials not to do so.

24. In approximately August 2016, as part of a standard background reinvestigation of SCHULTE for the purpose of renewing his security clearances, the CIA conducted interviews of multiple CIA Group colleagues. Among other things:

a. Some (but not all) colleagues independently reported that SCHULTE's demeanor with his management and colleagues, and his commitment to his work, changed markedly for the worse in or around February 2016.

b. Multiple colleagues stated that SCHULTE had indicated that he felt aggrieved by the CIA in a number of respects. Some also reported that they believed SCHULTE to be untrustworthy and potentially subject to outside coercion. (Other colleagues made no such report and, indeed affirmatively reported that they believed that SCHULTE was, in fact, trustworthy.)

c. Some (but not all) colleagues also reported that SCHULTE's security practices were lax, and that SCHULTE tended not to abide by security guidelines he deemed inconvenient—particularly guidelines concerning when and what kinds of media or data (such as external drives) could be connected or uploaded to CIA computer systems.⁷

H. SCHULTE's November 2016 Resignation from the CIA

25. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that, in connection with and preceding SCHULTE's November 2016 resignation from the CIA, he sent the following communications,

⁷ External drives can be connected to computers and files in order to allow users to move files from the computers onto the portable external drives.

among others:

a. Approximately one month prior to his resignation, on October 12, 2016, SCHULTE, using his CIA email account, sent an email to another CIA Group employee at that employee's official email account. The subject line of the email stated, "ROUGH DRAFT of Resignation Letter *EYES ONLY*." The email contained a letter entitled "Letter of Resignation 10/12/16" and addressed to "To whomever it may concern" ("Draft Resignation Letter"). I know from reviewing the Draft Resignation Letter, which spanned approximately three single-spaced pages, the following:

i. SCHULTE began the letter by stating, in substance and in part, that he had "always been a patriot" and would "obviously continue to support and defend this country until the day that I die," but that "from this day forward" he would "no longer do so as a public servant."

ii. SCHULTE claimed that he believed that the CIA Group management had unfairly "veiled" CIA leadership from various of SCHULTE's previously expressed concerns, including concerns about the network security of the CIA Group's LAN. SCHULTE continued: "That ends now. From this moment forward you can no longer claim ignorance; you can no longer pretend that you were not involved."

iii. SCHULTE explained that he was resigning from the CIA because CIA Group management had, among other things, "ignored" issues he had raised about "security concerns" and had attempted to "conceal these practices from senior leadership," including that the CIA Group's LAN was "incredibly vulnerable" to the theft of sensitive data. He claimed that one named CIA Group manager had ignored his security concerns and "later attempt[ed] to evade responsibility and blame the decentralized and insecure [CIA Group computing]

environment entirely on me.”⁸

iv. Specifically, SCHULTE wrote that inadequate CIA security measures had “left [the CIA Group’s LAN] open and easy for anyone to gain access and easily download [from the LAN] and upload [sensitive CIA Group computer code] in its entirety to the [public] internet.”

b. It appears that SCHULTE did not, in fact, submit the Draft Resignation Letter.

c. On his last day with the CIA (November 10, 2016), SCHULTE did, however, send an internal email to the CIA Office of the Inspector General (OIG) advising that office that he had been in contact with the United States House of Representatives’ Permanent Select Committee on Intelligence regarding his complaints about the CIA (“OIG Email”).

i. In the OIG Email, which SCHULTE labeled “Unclassified,” SCHULTE raised many of the same complaints included in the draft “Letter of Resignation 10/12/16,” described above, including the CIA’s treatment of him and its failure to address the “security concerns” he had repeatedly raised in the past.

ii. Shortly thereafter, CIA security learned that one of SCHULTE’s colleagues had witnessed SCHULTE printing the OIG Email, placing it in a folder, and exiting the CIA Component facility where SCHULTE worked.

iii. Notwithstanding SCHULTE’s labeling of the email as “Unclassified,” the CIA subsequently determined that the OIG Email which SCHULTE removed from the CIA without authorization did, in fact, contain classified information.

⁸ SCHULTE went on to describe other complaints he had about managers at the CIA. Among other things, SCHULTE described his complaints about the way in which CIA Group management had handled various personnel and disciplinary issues (*see supra* at Part II.G.16).

I. SCHULTE' s Use Of the Subject Google Account To Make Inquiries About the Status of the Investigation

26. Based on my conversations with other law enforcement agents and others, and my review of documents, I understand that, since the March 7, 2017 publication of the Classified Information on WikiLeaks, SCHULTE has repeatedly initiated contact, via telephone and text messages, with multiple of his former CIA Group colleagues. Those colleagues have reported that contact to government and law enforcement officials.

a. In those communications with his former colleagues, SCHULTE has repeatedly asked about the status of the investigation into the disclosure of the Classified Information.

b. SCHULTE has requested more details on the information that was disclosed.

c. SCHULTE has inquired of his interlocutors' personal opinions regarding who, within the CIA Group, each believes is responsible for the disclosure of the Classified Information. SCHULTE has also asked what other former CIA Group colleagues are saying about the disclosure.

d. SCHULTE has repeatedly denied any involvement in the disclosure of the Classified Information.

e. SCHULTE has indicated the he believes that he is a suspect in the investigation of the leak of Classified Information.

f. I am not aware of any other former CIA employee who has initiated any contact with former colleagues regarding the disclosure of the Classified Information.

27. Furthermore, I know that SCHULTE has specifically used the **Subject Google Account**, *i.e.*, the account associated with the Gmail account joshshulte1@gmail.com, to make

some of the inquiries described above. For example:

a. Records show that, on or about March 7, 2017, when WikiLeaks released the Classified Information, SCHULTE used the Google Voice feature associated with the **Subject Google Account** to send approximately 149 texts to multiple of his former colleagues at the CIA.

b. SCHULTE, using the Google Voice feature associated with the **Subject Google Account**, also had phone calls with former CIA colleagues, including one telephone call with a former colleague in which he, among other things, inquired of the former colleague's personal opinions regarding who was responsible for the disclosure of the Classified Information and what the person's motivation might be. SCHULTE indicated that he believed that the person responsible was a contractor who disclosed the Classified Information for fame.

c. In a call using the telephone number associated with the Subject Google Account on March 8, 2017 with the same former colleague, SCHULTE denied his involvement in the disclosure of the Classified Information, indicated his belief that many people suspected him of the disclosure, and relayed a conversation with another acquaintance in which SCHULTE had denied involvement in the disclosure of the Classified Information, but was dissatisfied with the acquaintance's reaction to SCHULTE's denial.

d. Records for recent communications on the Gmail feature of the Subject Google Account show that SCHULTE also continues to use various Google Services to communicate with others, including his Gmail address joshschulte1@gmail.com, which is listed as the recipient facility for several messages SCHULTE has received in the past two days. As discussed above, SCHULTE's account also reflects as recently as this month his enrollment in other Google Services, including Android, Google Docs, Google Drive, Google Groups, Google

Calendar, Google Hangouts, Google Payments, Google Photos, Google+, and Google Code.

J. The Subject Reddit Account and the Subject GitHub Account

28. Based on my conversations with other law enforcement agents and others, and my review of documents, I also know that references to SCHULTE in the context of the release of the Classified Information have been made on other websites, including those hosted by Reddit and GitHub. Specifically:

a. On or about March 7, 2017—i.e., the date of the release of the Classified Information by WikiLeaks—a “thread,” or online discussion, was opened by a Reddit user which was devoted to the release of the Classified Information.

b. As part of the thread, the user of the **Subject Reddit Account** made a post that stated: “What about this guy pedbsktbll?” (with the word “pedbsktbll” highlighted). The comment was followed by, among other things, (1) a listing of the following website: <https://github.com/pedbsktbll/projectwizard/blob/master/ProjectWizard/tempSubmodule.xml> (the “Website”) and (2) a line of text stating, “pedbsktbll - > Joshua Schulte.”

c. I know, based on a review of publicly available websites, including those available through various social media sites, that SCHULTE employs the user name “pedbsktbll” on various of these websites. For example, I know from reviewing a posting on the Google+ service associated with the Subject Google Account, which contains a photograph of SCHULTE, that SCHULTE listed various of his other social media accounts, several of which (e.g., including Facebook and Twitter) contain or reference the user name “pedbsktbll.”

29. I also know from viewing the Website, which features a page associated with the **Subject GitHub Account**, that the Webpage contains numerous lines of computer code, some of which reference computer applications that were referenced in the information released by WikiLeaks.

30. I respectfully submit that there is probable cause therefore to believe that the Target Accounts contain evidence, fruits, and instrumentalities of the Subject Offenses. Among other things, I respectfully submit that there is probable cause to establish that SCHULTE is proficient in and makes use of Internet-based computing services, like those offered by the Providers through the Target Accounts. Moreover, based on my training and experience, I know that individuals who engage in the Subject Offenses often use Internet-based services (like the Target Accounts) as a means by which to communicate with co-conspirators as well as means through which not only to transmit but also to store purloined information so that they do not have to carry it on their person. Finally, I know that individuals who engage in the Subject Offenses oftentimes use Internet-based computing services, like the Target Accounts, to publish purloined information. For example, based on my training and experience and my involvement in this investigation, I know that WikiLeaks is an Internet-based publication and that individuals who provide information to WikiLeaks in the past oftentimes have done so through the use of other Internet-based computing platforms, like the Target Accounts and other services offered by the Providers. Accordingly, when each of these factors is considered in conjunction with the fact of SCHULTE's access to the purloined information, his clear proficiency in computers and computer-programming, and the probable cause establishing SCHULTE's access to and use of the Subject Accounts, I respectfully submit that there is probably cause to believe that the Subject Accounts will contain evidence, fruits, and instrumentalities of the Subject Offenses.

K. SCHULTE's Planned Travel

31. Based on my conversations with other law enforcement agents and others, and my review of documents, including information provided by the Department of Homeland Security, I understand that SCHULTE has booked an international flight departing on Thursday, March 16, 2017. (Return travel to the United States is booked for a few days later.) The

aforementioned records and conversations reflect that this is only SCHULTE's second trip reflected in in DHS records outside the United States.

VI. Evidence, Fruits and Instrumentalities in Target Accounts

32. Based upon the foregoing, I respectfully submit there is probable cause to believe that information stored on the Providers' servers associated with the **Target Accounts** will contain evidence, fruits, and instrumentalities of the Subject Offenses, as more fully described in Section II of Attachment A to the requested warrants.

33. In particular, I believe the **Target Accounts** are likely to contain, among other things, the following information:

- a. Evidence of the identity(s) of the user(s) of the **Target Accounts** as well as other coconspirators in contact with the **Target Accounts**;
- b. Evidence relating to the participation in the Subject Offenses by the users of the **Target Accounts** and others, including information relating to the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials;
- c. Communications evidencing crimes, including but not limited to correspondence with others relating to the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials;
- d. Items, records or information consisting of, referring to, or reflecting classified documents or materials on the **Target Accounts**;
- e. Evidence concerning financial institutions and transactions used by the users of the **Target Accounts** in furtherance of the Subject Offenses;

- f. Evidence of and relating to computers or other online accounts and facilities (such as additional email addresses) controlled or maintained by the user of the **Target Accounts**;
- g. Passwords or other information needed to access any such computers, accounts, or facilities; and
- h. With respect to the Subject Google Account, evidence relating to the geolocation and travel of the user(s) of the **Target Accounts** at times relevant to the Subject Offenses.

34. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for service of a search warrant issued under § 2703, or for the collection or production of responsive records. Accordingly, the warrants requested herein will be transmitted to the Providers, which will be directed to produce a digital copy of any responsive records to law enforcement personnel within 10 days from the date of service. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will retain the records and review them for evidence, fruits, and instrumentalities of the Subject Offenses as specified in Section III of Attachment A to the requested warrants, which shall not be transmitted to the Providers.

35. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all content associated with the **Target Accounts**. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine

which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, to the extent applicable, including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.

VII. Request for Non-Disclosure and Sealing Orders

36. The existence and scope of this ongoing criminal investigation are not publicly known. As a result, premature public disclosure of this affidavit or the requested warrants could alert potential criminal targets that they are under investigation, causing them to destroy evidence, flee from prosecution, or otherwise seriously jeopardize the investigation. In particular, given that targets of the investigation are known to use computers and electronic communications in furtherance of their activity, the targets could easily delete, encrypt, or otherwise conceal such digital evidence from law enforcement were they to learn of the Government's investigation.

37. Accordingly, there is reason to believe that, were the Providers to notify the subscriber(s) or others of the existence of the requested warrants, the investigation would be seriously jeopardized. Pursuant to 18 U.S.C. § 2705(b), I therefore respectfully request that the

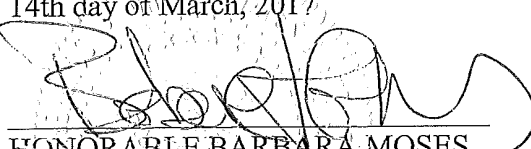
Court direct the Providers not to notify any person of the existence of the warrant for a period of 180 days from issuance, subject to extension upon application to the Court, if necessary.

38. For similar reasons, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter



Special Agent Jeff D. Donaldson
Federal Bureau of Investigation

Sworn to before me this
14th day of March, 2017


HONORABLE BARBARA MOSES
United States Magistrate Judge
Southern District of New York

17 MAG 6961

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All
Content and Other Information for the
Google account associated with Email
Address joshschulte1@gmail.com,
Maintained at Premises Controlled by
Google, Inc. and Google Payment
Corp.

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Google, Inc. and Google Payment Corp. (“Google”)

The Federal Bureau of Investigation (the “FBI” or the “Investigative Agency”)

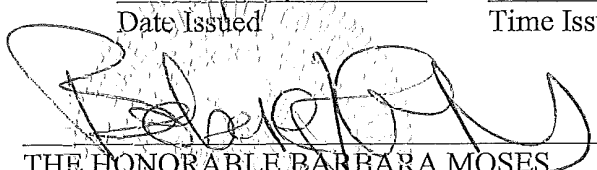
1. Warrant. Upon an affidavit of Special Agent of the FBI and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds that there is probable cause to believe that content information maintained at premises controlled by Google associated with the email address joshschulte1@gmail.com contains evidence, fruits, and instrumentalities of a crime, all as specified in Attachment A hereto. Accordingly, Google is hereby directed to provide to the Investigative Agency, within 10 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A, which shall not be transmitted to the Provider. The Government is required to serve a copy of this Warrant and Order on Google within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which Google is capable of accepting service.

2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, danger to the physical safety of an individual, flight from prosecution, and/or intimidation of potential witnesses or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that Google shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of 180 days from the date of this Order, subject to extension upon application to the Court if necessary, except that Google may disclose this Warrant and Order to an attorney for Google for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on Google; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

3/14/17 1:11 AM
 Date Issued Time Issued


 THE HONORABLE BARBARA MOSES
 United States Magistrate Judge
 southern District of New York

Attachment A

I. The Subject Account and Execution of Warrant

This warrant is directed to Google, Inc. and Google Payment Corp. (collectively, “Google” or the “Provider”) and applies to all content and other information within Google’s possession, custody, or control that is associated with the email address joshschulte1@gmail.com (the “Subject Gmail Account”).

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to Google. Google is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below, a copy of which shall not be transmitted to the Provider.

II. Information to be Produced by Google

To the extent it is within Google’s possession, custody, or control, Google is directed to produce the following information associated with the Subject Gmail Account:

a. Search History. All data concerning searches run by the user of the Subject Gmail Accounts, including, but not limited to, the content, date, and time of the search.

b. Google+ Photos and Content. All data concerning Google+ Photos, including all albums, photos, videos, and associated metadata for each file, as well as all Google+ posts, comments, profiles, contacts, and information relating to Google+ Circles.

c. Google Drive Content. All files and folders in the Google Drive associated with the Subject Gmail Account.

d. Google Voice. All records, voicemails, text messages, and other data associated with Google Voice.

e.

f. Google Wallet Content. All data and information in the Google Wallet associated with the Subject Gmail Account.

g. YouTube Content. For any YouTube account associated with the Subject Gmail Account, all subscriber information as well as copies of any videos and associated metadata and any YouTube comments or private messages.

h. Android Content. Any Android device information associated with the Subject Gmail Account, including IMEI/MEID, make and model, serial number, date and IP of last access to Google, and a list of all accounts that have ever been active on the device.

i. Email Content. All emails sent to or from, stored in draft form in, or otherwise associated with the Subject Gmail Account, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email).

j. Address book information. All address book, contact list, or similar information associated with the Subject Gmail Account.

k. Subscriber and payment information. All subscriber and payment information regarding the Subject Gmail Account, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

l. Linked accounts. The account identifiers for all accounts linked to the Subject Gmail Accounts, and subscriber records therefore as described in the preceding sub-paragraph,

including but not limited to any account linked to the Subject Gmail Account by registration IP address, “machine” or other cookie, alternate email address, or telephone number.

m. Transactional records. All transactional records associated with the Subject Gmail Account, including any IP logs or other records of session times and durations.

n. Customer correspondence. All correspondence with the subscriber or others associated with the Subject Gmail Account, including complaints, inquiries, or other contacts with support services and records of actions taken.

o. Preserved records. Any preserved copies of any of the foregoing categories of records created in response to any preservation request(s) issued pursuant to 18 U.S.C. § 2703(f).

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by Google in order to locate any evidence, fruits, and instrumentalities of violations (i) the unauthorized possession and, *inter alia*, the communication of national defense information to someone not entitled to receive it, in violation of Title 18, United States Code, Section 793(d); (ii) the unlawful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); (iii) exceeding authorized access to a computer in order to obtain national defense information with reason to believe that information could be used to the injury of the United States and the advantage of a foreign nation and willfully transmitting that information to a person not entitled to receive it, in violation of Title 18, United States Code, Section 1030(a)(1); and (iv) intentionally exceeding authorized access to a computer and thereby obtaining information from a department or agency of the United States,

in violation of Title 18, United States Code, Section 1030(a)(2)(B) (collectively the “Subject Offenses”), including the following:

- i. Evidence of the identity(s) of the user(s) of the Subject Gmail Account as well as other coconspirators in contact with the Subject Gmail Account;
- j. Evidence relating to the geolocation and travel of the user(s) of the Subject Gmail Account at times relevant to the Subject Offenses;
- k. Evidence relating to the participation in the Subject Offenses by the users of the Subject Gmail Account and others;
- l. Evidence concerning financial institutions and transactions used by the users of the Subject Gmail Account in furtherance of the Subject Offenses;
- m. Communications evidencing crimes, including but not limited to correspondence with others relating to the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials;
- n. Evidence of and relating to computers or other online accounts and facilities (such as additional email addresses) controlled or maintained by the user of the Subject Gmail Account; and
- o. Passwords or other information needed to access any such computers, accounts, or facilities.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

17 MAG 6961

In the Matter of a Warrant for All
Content and Other Information for the
Reddit, Inc. account associated with
account name L1347517, Maintained
at Premises Controlled by Reddit, Inc.

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Reddit, Inc.

The Federal Bureau of Investigation (the "FBI" or the "Investigative Agency")

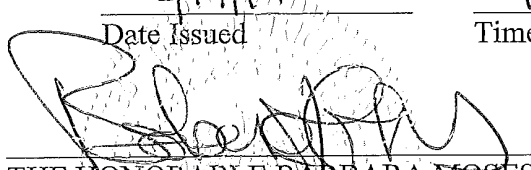
1. Warrant. Upon an affidavit of Special Agent of the FBI and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds that there is probable cause to believe that content information maintained at premises controlled by Reddit, Inc. associated with account name L1347517 contains evidence, fruits, and instrumentalities of a crime, all as specified in Attachment A hereto. Accordingly, Reddit, Inc. is hereby directed to provide to the Investigative Agency, within 10 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A, a copy of which shall not be transmitted to the Provider. The Government is required to serve a copy of this Warrant and Order on Reddit, Inc. within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which Reddit, Inc. is capable of accepting service.

2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or

tampering with evidence, danger to the physical safety of an individual, flight from prosecution, and/or intimidation of potential witnesses or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that Reddit, Inc. shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of 180 days from the date of this Order, subject to extension upon application to the Court if necessary, except that Reddit, Inc. may disclose this Warrant and Order to an attorney for Reddit, Inc. for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on Reddit, Inc.; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

<u>3/14/17</u> Date Issued	<u>1:12 AM</u> Time Issued
 _____ THE HONORABLE BARBARA MOSES United States Magistrate Judge southern District of New York	

Attachment A

I. The Subject Account and Execution of Warrant

This warrant is directed to Reddit, Inc. (the “Provider”) and applies to all content and other information within Reddit, Inc.’s possession, custody, or control that is associated with the account name L1347517 (the “Subject Account”).

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to Reddit, Inc. Reddit, Inc. is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below, a copy of which shall not be transmitted to the Provider.

II. Information to be Produced by Reddit, Inc.

To the extent it is within Reddit, Inc.’s possession, custody, or control, Reddit, Inc. is directed to produce the following information associated with the Subject Account:

a. Search History. All data concerning searches run, and posts accessed by the user of the Subject Account, including, but not limited to, the content, date, and time of the search or post access.

b. Post Content. All posts and messages made by the Subject Account, including all content, attachments, and any other information (specifically including the date and time at which each post or message was made/sent, and the size and length of each post/message).

c. Email Content or Direct Message Content. All emails and/or direct messages sent to or from, stored in draft form in, or otherwise associated with the Subject Account, including all message content, attachments, and header information (specifically including the source and

destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email).

d. Subscriber and payment information. All subscriber and payment information regarding the Subject Account, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

e. Transactional records. All transactional records associated with the Subject Account, including any IP logs or other records of session times and durations.

f. Customer correspondence. All correspondence with the subscriber or others associated with the Subject Account, including complaints, inquiries, or other contacts with support services and records of actions taken.

g. Preserved records. Any preserved copies of any of the foregoing categories of records created in response to any preservation request(s) issued pursuant to 18 U.S.C. § 2703(f).

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by Reddit, Inc. in order to locate any evidence, fruits, and instrumentalities of violations (i) the unauthorized possession and, *inter alia*, the communication of national defense information to someone not entitled to receive it, in violation of Title 18, United States Code, Section 793(d); (ii) the unlawful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); (iii) exceeding authorized access to a computer in order to obtain national defense information with reason to

believe that information could be used to the injury of the United States and the advantage of a foreign nation and willfully transmitting that information to a person not entitled to receive it, in violation of Title 18, United States Code, Section 1030(a)(1); and (iv) intentionally exceeding authorized access to a computer and thereby obtaining information from a department or agency of the United States, in violation of Title 18, United States Code, Section 1030(a)(2)(B) (collectively the “Subject Offenses”), including the following:

- p. Evidence of the identity(s) of the user(s) of the Subject Account as well as other coconspirators in contact with the Subject Account;
- q. Evidence relating to the geolocation and travel of the user(s) of the Subject Account at times relevant to the Subject Offenses;
- r. Evidence relating to the participation in the Subject Offenses by the users of the Subject Account and others;
- s. Evidence concerning financial institutions and transactions used by the users of the Subject Account in furtherance of the Subject Offenses;
- t. Communications evidencing crimes, including but not limited to correspondence with others relating to the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials;
- u. Evidence of and relating to computers or other online accounts and facilities (such as additional email addresses) controlled or maintained by the user of the Subject Account; and
- v. Passwords or other information needed to access any such computers, accounts, or facilities.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

17 MAG 6961

In the Matter of a Warrant for All
Content and Other Information for the
GitHub account associated with the
user name pedbsktbll, Maintained at
Premises Controlled by GitHub, Inc.

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: GitHub, Inc.

The Federal Bureau of Investigation (the “FBI” or the “Investigative Agency”)

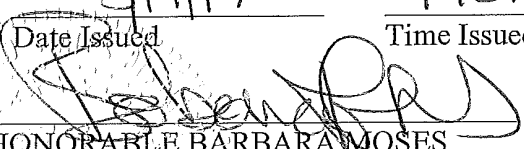
1. Warrant. Upon an affidavit of Special Agent of the FBI and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds that there is probable cause to believe that content information maintained at premises controlled by GitHub, Inc. associated with the user name pedbsktbll contains evidence, fruits, and instrumentalities of a crime, all as specified in Attachment A hereto. Accordingly, GitHub, Inc. is hereby directed to provide to the Investigative Agency, within 10 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A, a copy of which shall not be transmitted to the Provider. The Government is required to serve a copy of this Warrant and Order on GitHub, Inc. within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which GitHub, Inc. is capable of accepting service.

2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or

tampering with evidence, danger to the physical safety of an individual, flight from prosecution, and/or intimidation of potential witnesses or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that GitHub, Inc. shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of 180 days from the date of this Order, subject to extension upon application to the Court if necessary, except that GitHub, Inc. may disclose this Warrant and Order to an attorney for GitHub, Inc. for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on GitHub, Inc.; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

3/14/17 1:12 A.M.
 Date Issued Time Issued

 THE HONORABLE BARBARA MOSES
 United States Magistrate Judge
 southern District of New York

Attachment A

I. The Subject Account and Execution of Warrant

This warrant is directed to GitHub, Inc. (the “Provider”) and applies to all content and other information within GitHub, Inc.’s possession, custody, or control that is associated with the user name pedbsktbll (the “Subject Account”).

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to GitHub, Inc. GitHub, Inc. is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below, a copy of which shall not be transmitted to the Provider.

II. Information to be Produced by GitHub, Inc.

To the extent it is within GitHub, Inc.’s possession, custody, or control, GitHub, Inc. is directed to produce the following information associated with the Subject Account:

a. Use of GitHub Features. All features used by the Subject Account (*e.g.*, code review, project management, integrations, community management, documentation, code hosting, productivity tools). With respect to each feature used by the Subject Account, provide all data posted by or associated with the Subject Account.

b. GitHub Platforms. All platforms used by the Subject Account (*e.g.*, Atom, Electron, GitHub Desktop). With respect to each platform used by the Subject Account, provide all data posted by or associated with the Subject Account.

c. GitHub Repositories. All data from GitHub repositories that were posted by or associated with the Subject Account.

d. Email Content or Direct Message Content. All emails or direct messages sent to or from, stored in draft form in, or otherwise associated with the Subject Account, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email).

e. Address book information. All address book, contact list, or similar information associated with the Subject Account.

f. Subscriber and payment information. All subscriber and payment information regarding the Subject Account, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

g. Transactional records. All transactional records associated with the Subject Account, including any IP logs or other records of session times and durations.

h. Customer correspondence. All correspondence with the subscriber or others associated with the Subject Account, including complaints, inquiries, or other contacts with support services and records of actions taken.

i. Preserved records. Any preserved copies of any of the foregoing categories of records created in response to any preservation request(s) issued pursuant to 18 U.S.C. § 2703(f).

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by GitHub, Inc. in order to locate any evidence, fruits,

and instrumentalities of violations (i) the unauthorized possession and, *inter alia*, the communication of national defense information to someone not entitled to receive it, in violation of Title 18, United States Code, Section 793(d); (ii) the unlawful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); (iii) exceeding authorized access to a computer in order to obtain national defense information with reason to believe that information could be used to the injury of the United States and the advantage of a foreign nation and willfully transmitting that information to a person not entitled to receive it, in violation of Title 18, United States Code, Section 1030(a)(1); and (iv) intentionally exceeding authorized access to a computer and thereby obtaining information from a department or agency of the United States, in violation of Title 18, United States Code, Section 1030(a)(2)(B) (collectively the “Subject Offenses”), including the following:

- w. Evidence of the identity(s) of the user(s) of the Subject Account as well as other coconspirators in contact with the Subject Account;
- x. Evidence relating to the participation in the Subject Offenses by the users of the Subject Account and others;
- y. Evidence concerning financial institutions and transactions used by the users of the Subject Account in furtherance of the Subject Offenses;
- z. Communications evidencing crimes, including but not limited to correspondence with others relating to the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials;

- aa. Evidence of and relating to computers or other online accounts and facilities (such as additional email addresses) controlled or maintained by the user of the Subject Account; and
- bb. Passwords or other information needed to access any such computers, accounts, or facilities.

UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

MAR 14 2017

UNDER SEAL

In the Matter of the Search of
*(Briefly describe the property to be searched
 or identify the person by name and address)*
 Electronic Devices Previously Seized from the
 Premises of 200 East 39th Street, Apartment 8C,
 New York, NY 10016

Case No. 1:17-SW-199

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Electronic devices located at a U.S. Government facility in Herndon, Virginia,

located in the Eastern District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. 2252	Possession and production of sexually explicit material relating to children;
18 U.S.C. 2252A	Activities relating to material containing child pornography;
17/18 U.S.C. 506/2319	Criminal infringement of a copyright

The application is based on these facts:

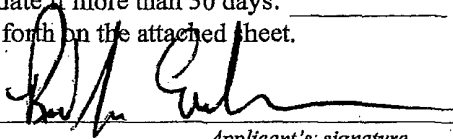
SEE ATTACHED AFFIDAVIT

☒ Continued on the attached sheet.

☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA/SAUSA:

AUSA Neil Hammerstrom



 Applicant's signature

Richard J. Evanchec, FBI Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 04/14/2017

/s/

 Theresa Carroll Buchanan
 United States Magistrate Judge

Judge's signature

City and state: Alexandria, Virginia

Theresa C. Buchanan, United States Magistrate Judge

Printed name and title

JAS_000143

JAS_027157

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

APR 14 2017

IN THE MATTER OF THE SEARCH OF:)
Electronic Devices Previously Seized from the)
Premises of 200 East 39th Street, Apartment 8C,)
New York, NY 10016)

UNDER SEAL

Case No. 1:17-SW- 199

AFFIDAVIT IN SUPPORT OF A SEARCH AND SEIZURE WARRANT

I, Richard J. Evanchec, being duly sworn, hereby deposes and says:

I. Introduction

A. Affiant

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI") assigned to the New York Field Office, and I have been employed by the FBI since 2004. I am currently assigned to a squad responsible for counterespionage matters and have worked in the field of counterintelligence from 2008 to present. In the course of my duties as a Special Agent, I am responsible for investigating offenses involving espionage and related violations of law, including unauthorized retention, gathering, transmitting or losing classified documents or materials; unauthorized removal and retention of classified documents or materials; illegally acting in the United States as a foreign agent; other national security offenses; and the making of false statements. As a result of my involvement in espionage investigations and investigations involving the unauthorized disclosure or retention of classified information, as well as my training in counterintelligence operations, I am familiar with the tactics, methods, and techniques of United States persons who possess, or have possessed a United States Government security clearance and may choose to harm the United States by misusing their access to classified information. I am also

familiar, though my training and experience, with the use of computers in criminal activity and the forensic analysis of electronically stored information.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the electronic devices specified below (“Subject Devices”) for the items and information described in Attachment A. Specifically, and as discussed in detail below, the Subject Devices were previously seized and searched pursuant to a separate warrant defined herein as the “Schulte Search Warrant,” and which was issued in connection with an investigation into the unlawful dissemination of classified materials.

3. While searching the Subject Devices for evidence, fruits, and instrumentalities of the offenses set forth in the Schulte Search Warrant, law enforcement officers encountered what appears to be an image of child pornography on one of the Subject Devices. Upon discovery of this suspected image of child pornography, the FBI promptly contacted the Assistant United States Attorneys involved in this investigation to inform them of this development, and the decision was made to seek additional authorization under Rule 41 of the Federal Rules of Criminal Procedure to search the Subject Devices for evidence, fruits, and instrumentalities of offenses involving child pornography, as specified below.

4. Similarly, while searching the Subject Devices for evidence, fruits, and instrumentalities of the offenses set forth in the Schulte Search Warrant, law enforcement officers also encountered what appears to be evidence of copyright infringement—specifically, the illegal streaming of dozens of movies—on one of the Subject Devices. Upon discovery of this evidence, the FBI also promptly contacted the Assistant United States Attorneys involved in this investigation to inform them of this development, and the decision was made to seek additional authorization under Rule 41 of the Federal Rules of Criminal Procedure to search the Subject

Devices for evidence, fruits, and instrumentalities of offenses involving copyright infringement, as specified below.

5. This Affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information ("ESI"). Because this Affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. The Subject Offenses

6. For the reasons detailed below, I believe that there is probable cause to believe that the Subject Devices also contain evidence, fruits, and instrumentalities of (i) violations of Title 18, United States Code, Section 2252 (possession, transportation, receipt, distribution, production, and reproduction of sexually explicit material relating to children) and Title 18, United States Code, Section 2252A (activities relating to material constituting or containing child pornography) (the "CP Offenses"); and (ii) violations of Title 17, United States Code, Section 506 and Title 18, United States Code, Section 2319 (criminal infringement of a copyright) (the "Copyright Offenses").

C. Terminology

7. The term "computer," as used herein, is defined as set forth in Title 18, United States Code, Section 1030(e)(1).

8. The terms "records," "documents," and "materials" include all information recorded in any form, visual or oral, and by any means, whether in handmade form (including, but

not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical discs, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device), as well as the equipment needed to record such information (including but not limited to cameras and video recording and storage devices).

9. The term child pornography is defined in Title 18, United States Code, Section 2256(8) in pertinent part as “any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where . . . the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct.”¹

10. The terms “Minor,” “Sexually Explicit Conduct” and “Visual Depiction” are defined as set forth in Title 18, United States Code, Section 2256.

II. Probable Cause Justifying Search of the Subject Devices

A. Probable Cause for Evidence of CP Offenses

11. On March 13, 2017, the Honorable Barbara C. Moses, a U.S. Magistrate Judge for the Southern District of New York, issued a search warrant (the “Schulte Search Warrant”) to

¹ See also *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002) (analyzing constitutional validity of the definitions set forth in 18 U.S.C. § 2256(8)).

search the residence of JOSHUA ADAM SCHULTE located at 200 East 39th Street, Apartment 8C, New York, New York 10016 (the “Residence”).² The Schulte Search Warrant was issued in connection with the investigation of the unauthorized dissemination on March 7, 2017, by wikileaks.org of documents and files that contained classified, national defense information belonging to the Central Intelligence Agency (the “Classified Materials”). As a result, the Schulte Search Warrant authorized the search of the Premises and any electronic devices found therein, for evidence, fruits, and instrumentalities of offenses relating to the unauthorized disclosure of the Classified Materials (the “Espionage Offenses”).

12. On or about March 15, 2017, members of the FBI searched the Residence.³ During the course of that search, law enforcement officers recovered, among other things, the Subject Devices, including multiple computers, servers, and other portable electronic storage devices.⁴ Following the seizure of the Subject Devices, the devices were transported by the FBI for analysis and examination to a U.S. Government facility in Herndon, Virginia, within the Eastern District of Virginia, where they remain as of the date of this application.

13. Based on my conversations with members of the FBI who are involved in searching the Subject Devices for evidence, fruits, and instrumentalities of the Espionage Offenses pursuant to the terms of the Schulte Search Warrant, I have learned, among other things, that on or about April 7, 2017, a photograph was discovered on SCHULTE’s desktop computer (the “Desktop

² A copy of the Schulte Search Warrant is attached as Exhibit A. A copy of the Affidavit in support of the Schulte Search Warrant is attached as Exhibit B and is incorporated herein by reference.

³ The March 15, 2017 search of the Residence was pursuant to a second search warrant issued by the Honorable Barbara C. Moses on the same day as the search. The Government sought a second search warrant because the Schulte Search Warrant was executed covertly on or about March 14, 2017. However, the items to be searched and seized pursuant to the second search warrant were identical to that which is set forth in the Schulte Search Warrant attached to this Affidavit.

⁴ A list of the Subject Devices is attached as Exhibit C.

Computer”) that appears to depict child pornography (the “CP Picture”). The Desktop Computer appears to have been connected to other Subject Devices in the Residence, including several servers. As a result, data on the Desktop Computer was likely also accessible through, or available on, some of the other Subject Devices in the Residence.

14. Based on my conversations with FBI agents who have spoken to an agent who is assigned to the Crimes Against Children Squad (the “CACS Agent”) and who has reviewed the CP Picture, I understand that the CP Picture appears to depict child pornography.⁵ Specifically, the CACS Agent believes the CP Picture depicts a naked young child on all fours and what appear to be two adults around her, one of whom appears to be performing a sexual act on the child—oral sex around the child’s buttocks. The CACS Agent also believes that the child is a minor based on, among other things, body structure, lack of breast development, and lack of pubic hair.

15. On or about March 14, 2017, pursuant to a search warrant authorized by the Honorable Barbara C. Moses, Google, Inc. produced information, including a history of JOSHUA ADAM SCHULTE’s Google searches (the “Google Search(es)”). Based on my review of those Google Searches, I have learned, among other things, that on a number of occasions in or about 2011 and in or about 2012, SCHULTE appears to have searched the Internet for child pornography. For example: (i) on or about April 9, 2011, SCHULTE conducted a Google Search for “child pornography” on at least three occasions; (ii) on or about October 15, 2011, SCHULTE conducted Google Searches for “movie where father videos daughter and friend sex” and “movie where father

⁵ Based on my conversations with the CACS Agent, I understand that it is possible that the CP Picture (like many photographs of child pornography) could be altered and not a real picture. However, the CACS Agent had only reviewed a printout of the CP Picture. Members of the FBI who analyzed the Desktop Computer have informed me that the CP Picture looks more like an actual photo when viewed on the computer as opposed to when printed. I have viewed the CP Picture on the Desktop Computer and believe that it is an actual photograph.

videos child porn”; and (iii) on or about May 15, 2012, SCHULTE conducted a Google Search for “female teenage body by year.”

16. Based on my training, experience, and discussions with other FBI agents, I know that persons who collect and distribute child pornography frequently collect and view sexually explicit materials in a variety of media, such as photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media that they use for their own sexual arousal and gratification. These examples of visual media containing sexually explicit materials are often times stored on various devices, such as the Subject Devices, including but not limited to, computers, disk drives, servers, modems, thumb drives, personal digital assistants, mobile phones and smart phones, digital cameras, and scanners, and the data within the aforesaid objects relating to said materials.

17. In addition, I know that individuals who collect and distribute child pornography, in the event that they change computers, will often back up or transfer files from their old computers’ hard drives to that of their new computers, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity. In addition, individuals who engage in such criminal activity will often also store or transfer files on electronic storage media other than computer hard drives, including thumb drives, flash memory cards, CD-ROMs, or portable hard drives to, for example, facilitate the use of the information or to transfer it to co-conspirators in support of the criminal scheme.

18. I also know that the child pornography detailed above was likely downloaded via the Internet using the Desktop Computer or other of the Subject Devices. As a result, the Desktop Computer and other Subject Devices may contain messages, emails, photographs, and/or videos relating to the possession, receipt, or production of child pornography. Computer files or remnants

of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files can be stored on a hard drive for years at little or no cost. Even when such files have been deleted, they can often be recovered, depending on how the hard drive has subsequently been used, months or years later with forensics tools. Specifically, when a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Deleted files, or remnants of deleted files, may accordingly reside in "slack space" (space that is not being used for storage of a file) for long periods of time before they are overwritten. In addition, a computer's operating system may keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are generally automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve from a hard drive or other electronic storage media depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

19. Based on the foregoing, I respectfully submit there is probable cause to believe that JOSHUA ADAM SCHULTE has engaged in the CP Offenses, and that evidence of this criminal activity is likely to be found on the Subject Devices. As a result, I am seeking authorization for a search warrant to search the Subject Devices for evidence of the CP Offenses. This includes, as set forth in Attachment A, the following:

- Evidence of computer programs used to access, transmit, or store information relating to the CP Offenses;
- Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from computer devices, storage media, and related electronic equipment;

- Evidence of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
- Motion pictures, films, videos, and other recordings of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
- Correspondence and records pertaining to violation of the CP Offenses including, but not limited to electronic mail, chat logs, electronic messages, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions involving any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
- Records or other items which evidence ownership, control, or use of, or access to computer devices, storage media, and related electronic equipment used to access, transmit, or store information relating to the CP Offenses, including but not limited to sales receipts, warranties, bills for internet access, registry entries, configuration files, saved usernames and passwords, user profiles, email contacts, and photographs.
- Information or correspondence pertaining to affiliation with any child exploitation bulletin boards, chat forums, or organizations;
- Any child pornography as defined by 18 U.S.C. § 2256(8);
- Any child erotica, defined as suggestive visual depictions of nude minors which do not constitute child pornography as defined by 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined by 18 U.S.C. § 2256(2);
- Notes, documents, records, invoices, or correspondence, in any format and medium, including, but not limited to, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);
- Names, and lists of names and addresses of individuals (including minors) related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);
- Mailing lists and/or supplier lists related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2); and
- Financial records, including credit card information, bills, and payment records related to related to the possession, distribution, receipt, or production of, or access with intent to

view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2)

20. This application also requests authorization to search the ESI on the Subject Devices pursuant to the same procedures as set forth in the Schulte Search Warrant. (*See* Schulte Search Warrant Application, Part IV.)

B. Probable Cause for Evidence of Copyright Offenses

21. Based on my conversations with members of the FBI who are involved in searching the Subject Devices for evidence, fruits, and instrumentalities of the Espionage Offenses pursuant to the terms of the Schulte Search Warrant, I have learned, among other things, that at least one of the servers recovered from the Residence ("Server-1") has indications that SCHULTE was involved in illegally sharing copyrighted movies over the Internet. Specifically, Server-1's command log (which shows the history of commands sent to Server-1 by the user, likely via a computer connected to Server-1), indicates that SCHULTE participated in the sharing of dozens of movies using "torrent trackers."⁶ Based on my training, experience and conversations with others, I understand that torrent trackers are computer code (or a "protocol") that connects computers on the Internet to each other in order to facilitate the transfer of large files over the Internet.

22. Based on my training, experience, and my review of the public catalog of copyrighted works available through the United States Copyright Office, I know that most, if not all, of the movies that SCHULTE appears to have participated in sharing are copyrighted works

⁶ Upon viewing the command log, which was searched pursuant to the terms of the Schulte Search Warrant for evidence regarding the Espionage Offenses, and upon seeing indications of illegal movie sharing, members of the FBI stopped viewing the command log and contacted the U.S. Attorney's Office.

registered with the United States Copyright Office. For example, among the many movies that were apparently shared include *Hacksaw Ridge*; *The Revenant*; *Captain America: Civil War*; and *The Hateful Eight*, all of which are copyrighted works currently registered with the United States Copyright Office.

23. In or about March 2017, FBI agents conducted interviews of multiple CIA employees who know SCHULTE. Among other things, one of those employees stated that SCHULTE operates a service allowing users to stream movies over the internet (the “Streaming Service”) and that SCHULTE manages the accounts of users of the Streaming Service.

24. Based on my review of a telephone that was among the Subject Devices for evidence, fruits, and instrumentalities of the Espionage Offenses pursuant to the terms of the Schulte Search Warrant, I have learned, among other things, that on or about October 31, 2016, SCHULTE sent an email to approximately 20 other individuals with the subject line “Pedbsktbll Plex Server Downtime 11/9/2016-1/2017” (the “Email”). In the Email, SCHULTE notifies the recipients that the “server will be down as it relocates to NYC starting 11/9. Thus, you will have the next 9 days to select and download material you may wish to watch during that downtime. Hopefully, the server will be back and running mid to late December – January at the latest.” Based on my training, experience, and participation in this investigation, I believe that SCHULTE was referring to the Streaming Service and was alerting users that the service would be unavailable while he moved to New York in late 2016.

25. Based on my training, experience, and discussions with other FBI agents, I know that persons who engage in the illegal transmission, distribution, and receipt of copyrighted works typically store evidence of such works on various devices, such as the Subject Devices, including but not limited to, computers, disk drives, servers, modems, thumb drives, personal

digital assistants, mobile phones and smart phones, digital cameras, and scanners, and the data within the aforesaid objects relating to said materials.

26. In addition, I know that individuals who engage in the illegal distribution of copyrighted works, in the event that they change computers, will often back up or transfer files from their old computers' hard drives to that of their new computers, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity. Furthermore, individuals who engage in such criminal activity will often also store or transfer files on electronic storage media other than computer hard drives, including thumb drives, flash memory cards, CD-ROMs, or portable hard drives to, for example, facilitate the use of the information or to transfer it to co-conspirators in support of the criminal scheme.

27. I also know that the movies detailed above were likely downloaded via the Internet using Server-1 and other of the Subject Devices. As a result, Server-1 and other Subject Devices may contain messages, emails, and/or videos relating to the transmission, distribution, and receipt of copyrighted works. As noted above, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet.

28. Based on the foregoing, I respectfully submit there is also probable cause to believe that JOSHUA ADAM SCHULTE has engaged in the Copyright Offenses, and that evidence of this criminal activity is likely to be found on the Subject Devices. I am also seeking authorization for a search warrant to search the Subject Devices for evidence of the Copyright Offenses. Specifically, this includes, as set forth in Attachment A, the following:

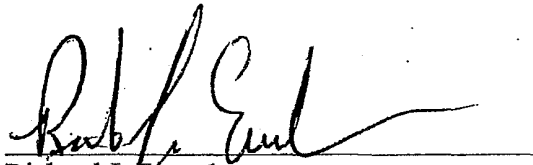
- Evidence of computer programs used to transmit or store information relating to the Copyright Offenses;

- Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from computer devices, storage media, and related electronic equipment;
- Evidence of copyrighted works, including motion pictures, films, videos, other recordings, and documents relating to the Copyright Offenses;
- Correspondence and records pertaining to violation of the Copyright Offenses including, but not limited to electronic mail, chat logs, electronic messages, and records bearing on the transmission, receipt, and/or storage of copyrighted works;
- Records or other items which evidence ownership, control, or use of, or access to computer devices, storage media, and related electronic equipment used to transmit or store information relating to the Copyright Offenses, including but not limited to sales receipts, warranties, bills for internet access, registry entries, configuration files, saved usernames and passwords, user profiles, email contacts, and photographs.
- Any copyrighted works;
- Notes, documents, records, invoices, or correspondence, in any format and medium, including, but not limited to, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, related to the transmission, receipt, and/or storage of copyrighted works;
- Names, and lists of names and addresses of individuals (including minors) related to the transmission, receipt, and/or storage of copyrighted works;
- Mailing lists and/or supplier lists related to the transmission, receipt, and/or storage of copyrighted works; and
- Financial records, including credit card information, bills, and payment records related to the transmission, receipt, and/or storage of copyrighted works.

29. This application also requests authorization to search the ESI on the Subject Devices pursuant to the same procedures as set forth in the Schulte Search Warrant. (See Schulte Search Warrant Application, Part IV.)

III. Conclusion and Ancillary Provisions

30. Based on the foregoing, I respectfully request the court to issue a warrant to search the items and information specified in Attachment A to this Affidavit and to the Search and Seizure Warrant. In light of the confidential nature of the continuing investigation, I respectfully request that this Affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise.



Richard J. Evanchec
Special Agent
Federal Bureau of Investigation

Sworn to and signed before me on
this 14th day of April 2017



/s/
Theresa Carroll Buchanan
United States Magistrate Judge

Theresa Carroll Buchanan
United States Magistrate Judge

Attachment A

I. Devices to be Searched—Subject Devices

The devices to be searched (the “Subject Devices”) include any and all electronic devices seized pursuant to a search warrant executed on or about March 15, 2017 at the premises described as apartment 8C in a building located at 200 East 39th Street, New York, New York 10016.

II. The Search of the Subject Devices

A. Evidence, Fruits, and Instrumentalities of the Child Pornography Offenses

The Subject Devices may be searched for the following evidence, fruits, and/or instrumentalities of violations of Title 18, United States Code, Sections 2252 (activities relating to material constituting or containing child pornography) and 2252A (possession, transportation, receipt, distribution, production, and reproduction of sexually explicit material relating to children) (the “CP Offenses”):

- Evidence of computer programs used to access, transmit, or store information relating to the CP Offenses;
- Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from computer devices, storage media, and related electronic equipment;
- Evidence of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
- Motion pictures, films, videos, and other recordings of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
- Correspondence and records pertaining to violation of the CP Offenses including, but not limited to electronic mail, chat logs, electronic messages, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions involving any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
- Records or other items which evidence ownership, control, or use of, or access to computer devices, storage media, and related electronic equipment used to access, transmit, or store information relating to the CP Offenses, including but not limited to sales receipts, warranties, bills for internet access, registry entries, configuration files, saved usernames and passwords, user profiles, email contacts, and photographs.

- Information or correspondence pertaining to affiliation with any child exploitation bulletin boards, chat forums, or organizations;
- Any child pornography as defined by 18 U.S.C. § 2256(8);
- Any child erotica, defined as suggestive visual depictions of nude minors which do not constitute child pornography as defined by 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined by 18 U.S.C. § 2256(2);
- Notes, documents, records, invoices, or correspondence, in any format and medium, including, but not limited to, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);
- Names, and lists of names and addresses of individuals (including minors) related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);
- Mailing lists and/or supplier lists related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2); and
- Financial records, including credit card information, bills, and payment records related to related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

B. Evidence, Fruits, and Instrumentalities of the Copyright Offenses

The Subject Devices may also be searched for the following evidence, fruits, and/or instrumentalities of violations of violations of 17 U.S.C. § 506 and 18 U.S.C. § 2319 (criminal infringement of a copyright) (the "Copyright Offenses"):

- Evidence of computer programs used to transmit or store information relating to the Copyright Offenses;
- Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from computer devices, storage media, and related electronic equipment;

- Evidence of copyrighted works, including motion pictures, films, videos, other recordings, and documents relating to the Copyright Offenses;
- Correspondence and records pertaining to violation of the Copyright Offenses including, but not limited to electronic mail, chat logs, electronic messages, and records bearing on the transmission, receipt, and/or storage of copyrighted works;
- Records or other items which evidence ownership, control, or use of, or access to computer devices, storage media, and related electronic equipment used to transmit or store information relating to the Copyright Offenses, including but not limited to sales receipts, warranties, bills for internet access, registry entries, configuration files, saved usernames and passwords, user profiles, email contacts, and photographs.
- Any copyrighted works;
- Notes, documents, records, invoices, or correspondence, in any format and medium, including, but not limited to, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, related to the transmission, receipt, and/or storage of copyrighted works;
- Names, and lists of names and addresses of individuals (including minors) related to the transmission, receipt, and/or storage of copyrighted works;
- Mailing lists and/or supplier lists related to the transmission, receipt, and/or storage of copyrighted works; and
- Financial records, including credit card information, bills, and payment records related to the transmission, receipt, and/or storage of copyrighted works.

C. Review of ESI

In conducting a review of ESI on the Subject Devices, law enforcement personnel may use various techniques, including but not limited to:

- surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few "pages" of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files;
- scanning storage areas for deliberately hidden files;

- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- making reasonable efforts to utilize computer search methodology to search only for files, documents, or other electronically stored information within the categories identified in Section II.A of this Attachment.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Section II.A of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all ESI from the Subject Devices if necessary to evaluate its contents and to locate all data responsive to the warrant.

EXHIBIT A

JAS_000162

JAS_027176

AO 93 (SDNY Rev. 01/17) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
Southern District of New YorkIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)200 East 39th Street, Apartment 8C, New York, New
York 10016, as well as Any Closed Containers/Items;
See Attachment A

Case No.

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Southern District of New York
(identify the person or describe the property to be searched and give its location):

200 East 39th Street, Apartment 8C, New York, New York 10016; see Attachment A

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property
to be seized):

See Attachment A

The search and seizure are related to violation(s) of (insert statutory citations):

18 U.S.C. 793(d), 793(e), 1030(a)(1), 1030(a)(2)(B).

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or
property.**YOU ARE COMMANDED** to execute this warrant on or before March 27, 2017

(not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10 p.m. ☒ at any time in the day or night as I find reasonable cause has been
established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property
taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the
place where the property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an
inventory as required by law and promptly return this warrant and inventory to the Clerk of the Court.☒ Upon its return, this warrant and inventory should be filed under seal by the Clerk of the Court. S/Barbara
USMJ Initials☒ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay
of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be
searched or seized (check the appropriate box) ☒ for 30 days (not to exceed 30).☐ until, the facts justifying, the later specific date of _____.

S/Barbara Moses

Date and time issued: MAR 13 2017 1:07

Judge's signature

City and state: New York, NY

Honorable Barbara C. Moses

Printed name and title

JAS_000163

JAS_027177

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
-----------	---------------------------------	--

Inventory of the property taken and name of any person(s) seized:

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the Court.

Date: _____

Executing officer's signature

Printed name and title

JAS_000164

JAS_027178

Attachment A

I. Premises to be Searched—Subject Premises

The premises to be searched (the “Subject Premises”) is described as follows, and includes all locked and closed containers found therein:

The Subject Premises is particularly described as apartment 8C in a building located at 200 East 39th Street, New York, New York 10016 (the “Building”). The Building is located near the corner of 39th Street and Third Avenue. The Building is nineteen stories high and contains approximately ninety-one apartment units. The Subject Premises is a one-bedroom apartment located on the eighth floor of the Building, and it is clearly identifiable as apartment 8C from the outside of the Subject Premises.

II. Execution of the Warrant

Law enforcement agents are permitted to execute the search warrant at any time in the day or night, and further to execute the search warrant covertly without advance or contemporaneous notice of the execution of the search warrant. Law enforcement agents will provide notice of the execution of the warrant within seven days of execution unless there is a new showing, made to the Court, that delayed notice is appropriate.

III. Items to Be Searched and Seized

A. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be searched and/or seized from the Subject Premises include the following evidence, fruits, and instrumentalities of: (i) the unauthorized possession and, *inter alia*, the communication of national defense information to someone not entitled to receive it, in violation of Title 18, United States Code, Section 793(d); (ii) the unlawful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); (iii) exceeding authorized access to a computer in order to obtain national defense information with reason to believe that information could be used to the injury of the United States and the advantage of a foreign nation and willfully transmitting that information to a person not entitled to receive it, in violation of Title

18, United States Code, Section 1030(a)(1); and (iv) intentionally exceeding authorized access and thereby obtaining information from a department or agency of the United States, in violation of Title 18, United States Code, Section 1030(a)(2)(B) (collectively, the “Subject Offenses”):

1. Evidence concerning occupancy or ownership of the Subject Premises, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys.

2. Evidence concerning the identity or location of, and communications with, any co-conspirators.

3. Any and all notes, documents, records, correspondence, or materials, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, and handwritten notes), pertaining to the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials.

4. Electronic devices (including but not limited to computers, tablets, smartphones, and cellular telephones) and storage media used in furtherance of the Subject Offenses, containing evidence of the Subject Offenses, or containing evidence authorized for seizure in paragraphs 1, 2 and 3 above. The term “storage media” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

5. Electronic forensic evidence relating to the Subject Offenses, including for any electronic device or storage media whose search and/or seizure is authorized by this warrant as described above in paragraph 4 (hereinafter, “Computers”¹), including:

- a. evidence of the times the Computers were used in furtherance of the Subject Offenses;
- b. passwords, encryption keys, and other access devices that may be necessary to access the Computers;
- c. documentation and manuals that may be necessary to access the Computers or to conduct a forensic examination of the Computers;
- d. evidence of software that would allow others to control the Computers, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- e. evidence indicating how and when the Computers were accessed or used in furtherance of the Subject Offenses;
- f. evidence indicating the Computers’ user’s/users’ state of mind as it relates to the Subject Offenses;
- g. evidence of the attachment to the Computers of other storage devices or similar containers for electronic evidence in furtherance of the Subject Offenses;

¹ The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

- h. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Computers;
- i. records of or information about Internet Protocol addresses used by the Computers;
- j. records of or information about the Computers' Internet activity in furtherance of the Subject Offenses, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

6. If law enforcement personnel seize the computer(s) or other electronic device(s), the personnel will search the computer and/or device(s) within a reasonable amount of time, not to exceed 60 days from the date of execution of the warrant. If, after such a search has been conducted, it is determined that a computer or device contains any data listed in paragraphs 1 through 3, the Government will retain the computer or device. If it is determined that the computer(s) or device(s) are no longer necessary to retrieve and preserve the data, and the items are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(b), such materials and/or equipment will be returned within a reasonable time. In any event, such materials and/or equipment shall be returned no later than 60 days from the execution of this warrant, unless further application is made to the Court.

B. Search and Seizure of Electronically Stored Information

The items to be searched and seized from the Subject Premises also include any computer devices and storage media that may contain any electronically stored information falling within the categories set forth in Section III.A of this Attachment above, including, but not limited to,

desktop and laptop computers, disk drives, modems, thumb drives, personal digital assistants, smart phones, digital cameras, and scanners. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

The items to be searched and seized from the Subject Premises also include:

1. Any items or records needed to access the data stored on any seized or copied computer devices or storage media, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.
2. Any items or records that may facilitate a forensic examination of the computer devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.
3. Any evidence concerning the persons with access to, control over, or ownership of the seized or copied computer devices or storage media.

C. Review of ESI

Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques, including but not limited to:

- surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few "pages" of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files;
- scanning storage areas for deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- making reasonable efforts to utilize computer search methodology to search only for files, documents, or other electronically stored information within the categories identified in Sections I.A and I.B of this Attachment.

EXHIBIT B

JAS_000171

JAS_027185

UNITED STATES DISTRICT COURT

for the
Southern District of New York

17 MAG 1856

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)200 East 39th Street, Apartment 8C, New York, New
York 10016, as well as Any Closed Containers/Items

Case No.

APPLICATION FOR A SEARCH AND SEIZURE WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

200 East 39th Street, Apartment 8C, New York, New York 10016

located in the Southern District of New York, there is now concealed (identify the person or describe the property to be seized):

See Attached Affidavit and its Attachment A

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section(s)	Offense Description(s)
18 U.S.C. 793(d), 793(e), 1030(a)(1), 1030(a)(2)(B).	Offenses relating to unauthorized possession and distribution of national defense information

The application is based on these facts:

See Attached Affidavit and its Attachment A

- ☒ Continued on the attached sheet.
☒ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me and signed in my presence.

Date: 03/13/2017City and state: New York, NY

Applicant's signature

Special Agent Jeff D. Donaldson, FBI

Printed name and title

S/Barbara Moses

Judge's signature

Honorable Barbara C. Moses

Printed name and title

JAS_000172

JAS_027186

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of the Application of the United States of America for a Search Warrant for the Premises Known and Described as 200 East 39th Street, Apartment 8C, New York, New York 10016, as well as Any Closed Containers/Items Contained in the Premises

TO BE FILED UNDER SEAL

**Agent Affidavit in Support of
Application for Search Warrant**

SOUTHERN DISTRICT OF NEW YORK) ss.:

JEFF D. DONALDSON, being duly sworn, deposes and says:

I. Introduction

A. Affiant

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI") assigned to the New York Field Office, and have been employed by the FBI since 2010. I am currently assigned to a squad responsible for counterespionage matters and have worked in the field of counterintelligence from 2010 to present. In the course of my duties as a Special Agent, I am responsible for investigating offenses involving espionage and related violations of law, including unauthorized retention, gathering, transmitting or losing classified documents or materials; unauthorized removal and retention of classified documents or materials; illegally acting in the United States as a foreign agent; other national security offenses; and the making of false statements. As a result of my involvement in espionage investigations and investigations involving the unauthorized disclosure or retention of classified information, as well as my training in counterintelligence operations, I am familiar with the tactics, methods, and techniques of United States persons who possess, or have possessed a United States Government security clearance and may choose to harm the United States by misusing their access to classified information. I am also

familiar, though my training and experience with the use of computers in criminal activity and the forensic analysis of electronically stored information.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises specified below (“Subject Premises”) for the items and information described in Attachment A. This Affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information (“ESI”). Because this Affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. The Subject Premises

3. The Subject Premises is particularly described as apartment 8C in a residential apartment building located at 200 East 39th Street, New York, New York 10016 (the “Building”). The Building is located near the corner of 39th Street and Third Avenue in Manhattan. The Building is nineteen stories high and contains approximately ninety-one apartment units. The Subject Premises is a one-bedroom apartment located on the eighth floor of the Building, and it is clearly identifiable as Apartment 8C from the outside of the Subject Premises.

C. The Subject Offenses

4. For the reasons detailed below, I believe that there is probable cause to believe that the Subject Premises contain evidence, fruits, and instrumentalities of (i) the unauthorized possession and, *inter alia*, the communication of national defense information to someone not entitled to receive it, in violation of Title 18, United States Code, Section 793(d); (ii) the unlawful

retention of national defense information, in violation of Title 18, United States Code, Section 793(e); (iii) exceeding authorized access to a computer in order to obtain national defense information with reason to believe that information could be used to the injury of the United States and the advantage of a foreign nation and willfully transmitting that information to a person not entitled to receive it, in violation of Title 18, United States Code, Section 1030(a)(1); and (iv) intentionally exceeding authorized access to a computer and thereby obtaining information from a department or agency of the United States, in violation of Title 18, United States Code, Section 1030(a)(2)(B) (collectively the “Subject Offenses”).

D. Terminology

5. The term “computer,” as used herein, is defined as set forth in 18 U.S.C. § 1030(e)(1).

6. The terms “records,” “documents,” and “materials” include all information recorded in any form, visual or oral, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical discs, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device), as well as the equipment needed to record such information (including but not limited to cameras and video recording and storage devices).

II. Probable Cause

A. WikiLeaks Publication of Classified CIA Information

7. Based on my review of publicly available material on the Internet, including on the website wikileaks.org (“WikiLeaks”), I know that, on March 7, 2017, WikiLeaks published what it claimed were more than 8,000 documents and files that contained classified information (the “Classified Information”) belonging to the Central Intelligence Agency (“CIA”). In its press release accompanying the Classified Information, WikiLeaks further claimed that:

a. The public dissemination of the Classified Information was “the largest ever” unauthorized publication of classified CIA documents.

b. The Classified Information constituted the “first full part” of a series—thus indicating that there would be subsequent publications of additional sensitive CIA information.

c. The “collection” obtained by WikiLeaks amounted to “more than several hundred million lines of code” and revealed the “entire hacking capacity” of the CIA, including various malware, viruses, and other tools used by the CIA.

8. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that:

a. The information that WikiLeaks claimed was classified CIA information—that is, the Classified Information—was at the time of its disclosure, in fact, classified CIA information.

b. Specifically, the Classified Information was created and maintained by one specific group within the CIA which is responsible for various computer engineering activities, including the development of computer code (the “CIA Group”). That CIA Group exists within a larger CIA component (the “CIA Component”). In March 2016, less than 200 employees were assigned to the CIA Group. And only employees of the CIA Group had access to the computer

network on which the Classified Information that was stolen from the CIA Group's computer network was stored. (Moreover, as described in detail below, only three of those approximately 200 people who worked for the CIA Group had access to the specific portion of the Group's computer network on which the Classified Information was likely stored.)

c. The Classified Information appears to have been stolen from the CIA Component sometime between the night of March 7, 2016 and the night of March 8, 2016.

i. This is based on preliminary analysis of the timestamps associated with the Classified Information which indicates that March 7, 2016 was the latest (or most recent) creation or modification date associated with the Classified Information.

ii. Because, for the reasons described below (*see infra* Part C.10), the Classified Information was apparently copied from an automated daily back-up file, it is likely that the Classified Information was copied either late on March 7, 2016 (after the March 7 nightly back-up was completed) or on March 8, 2016 (before the March 8 nightly back-up was completed).

iii. This is so because if the Classified Information was copied before the March 7 back-up, one would *not* expect to see in the Classified Information documents dated as late as March 7. And if the Classified Information was copied after the March 8 back-up, one *would* expect to see documents dated on or after March 8 because the "back-ups" occur approximately each day.¹

¹ It is of course possible that the Classified Information was copied later than March 8, 2016 even though the creation/modification dates associated with it appear to end on March 7, 2016. For example, the individual who copied and removed the data could have limited his or her copying to data that was modified or created on or before March 7, 2016. (Conversely, however, the Classified Information is unlikely to have been copied before March 7, 2016, because it contains data that was created as recently as March 7, 2016.) Because the most recent timestamp on the Classified Information reflects a date of March 7, 2016, preliminary analysis indicates that the Classified Information was likely copied between the end of the day on March 7 and the end of the day on March 8.

d. The Classified Information was publicly released by WikiLeaks exactly one year to the day (March 7, 2017) from the latest date associated with the Classified Information (March 7, 2016).

e. The duplication and removal from the CIA Group's computer network of the Classified Information and its subsequent public dissemination via WikiLeaks was not authorized by the United States government.

f. The unauthorized disclosure of the Classified Information could—at a minimum—reasonably be expected to cause serious damage to the national security of the United States. *See* Executive Order 13526; 18 C.F.R. § 3a.11(a)(2).

g. The Classified Information is national defense information and its disclosure could reasonably be expected to be used to the injury to the United States and to the advantage of a foreign nation. *See* 18 U.S.C. § 793(d) & (e).

B. The CIA Group's Local Area Computer Network (LAN) and Back-Up Server

9. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that the Classified Information originated in a specific isolated local area computer network ("LAN") used exclusively by the CIA Group.² As described above, in and around March 2016, in total less than 200 people had access to the CIA Group's LAN on which the Classified Information was stored.

a. An isolated network, such as the CIA Group's LAN, is a network-security structure by which the isolated network is physically separated (or "air-gapped") from unsecured networks, such as the public Internet.

² In its press release announcing the publication of the Classified Information, WikiLeaks stated that the Classified Information originated from "an isolated, high-security network."

b. Accordingly, such isolated networks, like the LAN, cannot be accessed from the public Internet, but rather only through those computers which are physically connected to the isolated network.

c. The CIA Group's LAN, and each of its component parts, was maintained in heavily physically secured governmental facilities, which include multiple access controls and various other security measures.

d. The isolated LAN used by the CIA Group was comprised of multiple networked computers and servers. (Each of these component computers and servers were, by definition, inside the electronically isolated LAN.)

i. In order to preserve and protect the CIA Group employees' day-to-day computer engineering work, that work was backed up, on an approximately daily basis, to another server on the CIA Group's LAN that was used to store back-up data (the "Back-Up Server").

ii. Back-ups of the sort stored on the Back-Up Server are designed to ensure that, should the original data be corrupted or deleted, the stored data is not lost, but rather—because of the daily back-ups—is maintained via the daily copies stored on the Back-Up Server.

C. The Publicly Disclosed Classified Information Likely Originated on the CIA Group's Back-Up Server

10. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I understand that the Classified Information that was publicly released by WikiLeaks appears likely to have been copied—specifically—from the CIA Group's Back-Up Server.

a. As described above, the Back-Up Server served as a secondary storage location for data that principally resided on the primary computer network used for CIA Group

employees' day-to-day work writing computer code. Approximately each day, an automated process would back-up that data to the Back-Up Server. Each of those daily back-ups was akin to an electronic "snapshot" of the data on that particular date. In that way, the Back-Up Server simultaneously acquired and stored, on a rolling basis, daily snapshots of the original data.

b. As such, if the data contained on the Back-Up Server was copied *en masse* directly from that Server, the copy would contain numerous iterations (or snapshots) of the similar or same data which had been backed up from the original data, distinguished by date.

c. The publicly released Classified Information does in fact contain numerous iterations (or snapshots) of the similar or same data, distinguished by date.

d. Accordingly, the fact that the Classified Information contains numerous iterations (or snapshots) of the similar or same data, distinguished by date, is strongly supportive of the fact that the Classified Information was taken from the CIA Group's Back-Up Server.³

e. As described above (*see supra* Part II.A.8.c), because the most recent timestamp associated with the Classified Information appears to be March 7, 2016, it is likely that the Classified Information was copied from the Back-Up Server after the daily back-up on March 7, 2016, and before the daily back-up on March 8, 2016.

D. TARGET SUBJECT JOSHUA ADAM SCHULTE Was One of Only Three Employees Across the Entire CIA Who, in March 2016, Had Been Given System Administrator Access To the Back-Up Server

11. Based on my conversations with other law enforcement agents and others, my

³ I understand, based on my conversations with others familiar with the CIA Group's LAN that it would be difficult, if not impossible, to copy from the data (not on the Back-Up Server) the multiple different date-distinguished iterations of the same data that are included in the publicly released Classified Information. In contrast, a single copy of the Back-Up Server would likely include each of the prior iterations (or snapshots) of the same data—which is exactly what is reflected in the publicly released Classified Information.

review of documents, and my training and experience, I know that the CIA Group's LAN was designed such that only those employees who were specifically given a particular type of systems-administrator access ("Systems Administrators") could access the Back-Up Server.

a. Systems Administrators were given a particular username and password in order to log on to and access the Back-Up Server.

b. Conversely, CIA employees who were not designated Systems Administrators were not given access to the Back-Up Server.⁴

12. I know, based on my conversations with other law enforcement agents and others, in approximately March 2016—the month when the Classified Information is assessed to have been copied—only three CIA employees were designated Systems Administrators with access to the CIA Group's Back-Up Server.

a. TARGET SUBJECT JOSHUA ADAM SCHULTE ("SCHULTE") was one of those three Systems Administrators.

i. SCHULTE was employed as a computer engineer by the CIA—specifically in the CIA Group—from in or about May 2010 through on or about November 10, 2016, when he resigned from the CIA.

ii. During SCHULTE's more than six years working in the CIA Group, his responsibilities included, among other things, developing computer code for specific projects, including projects explicitly described in the Classified Information.

⁴ It is, of course, possible that an employee who was not a designated Systems Administrator could find a way to gain access to the Back-Up Server. For example, such an employee could steal and use—without legitimate authorization—the username and password of a designated Systems Administrator. Or an employee lacking Systems Administrator access could, at least theoretically, gain access to the Back-Up Server by finding a "back- door" into the Back-Up Server.

iii. SCHULTE had a skill set that enabled him to write computer code designed to clandestinely copy data from computers.

b. As described above, in March 2016, SCHULTE was one of only three CIA employees throughout the entire CIA who had authorized access to the CIA Group's Back-Up Server from which the Classified Information was likely copied. The publicly released Classified Information published by WikiLeaks, based on a preliminary review, appears to contain the names and/or pseudonyms of, *inter alia*, multiple CIA employees—including two of the three aforementioned individuals with designated Systems Administrator privileges.

i. Names used by the other two CIA Group Systems Administrators were, in fact, published in the publicly released Classified Information.

ii. SCHULTE's name, on the other hand, was not apparently published in the Classified Information.

iii. Thus, SCHULTE was the only one of the three Systems Administrators with access to the Classified Information on the Back-Up Server who was not publicly identified via WikiLeaks's publication of the Classified Information.

c. The other two individuals who served in March 2016 as Systems Administrators for the CIA Group's LAN remain employed by the CIA. SCHULTE resigned from the CIA in November 2016, as described in detail below.

E. SCHULTE Had Access to the Back-Up Server on March 7 and 8, 2016—The Likely Dates of the Copying of the Classified Information

13. As described above (see *supra* Part II.C.10), it appears likely that the Classified Information was copied between March 7 and March 8, 2016.

a. Based on my conversations with other law enforcement agents and others, and my review of documents, including access records of the CIA Component facility in which

SCHULTE worked, I know that he was present at work from approximately:

- i. 10:01 a.m. until 7:16 p.m. on March 7, 2016; and
- ii. 10:19 a.m. until 7:40 p.m. on March 8, 2016.

b. Based on my conversations with other law enforcement agents and others, and my review of documents, I know that on March 8, 2016, the CIA Group held an offsite management retreat for many of its senior and midlevel managers. Accordingly, on March 8th, much of the CIA Group's management, including some to whom SCHULTE reported, were not present in the CIA Component building where SCHULTE and other CIA Group employees worked.

c. I further understand that SCHULTE's workspace (*i.e.*, his desk and computer workstation) was set up such that only three other CIA Group Employees had direct line-of-sight to SCHULTE's desk and computer—that is, only three other employees could see what he was doing at his desk. At least two of those three employees were at the offsite management retreat on March 8, 2016.

d. As described above, in March 2016, only two CIA employees in addition to SCHULTE were designated Systems Administrators with access to the CIA Group's Back-Up Server from which the Classified Information was likely copied. On March 8, 2016, one of those two other designated Systems Administrators was at the offsite management retreat. (The retreat was held at a location that did not have any access to the CIA Group's LAN, including the Back-up Server, and therefore afforded no access to the Classified Information.)⁵

⁵ On March 7 and 8, 2016, the third of the three CIA employees with Systems Administrator access was located at a CIA facility that did, in fact, have access to the Back-Up Server from which the Classified Information was likely copied.

F. SCHULTE's Unauthorized Unilateral Reinstatement of His Own Administrative Privileges

14. Based on my conversations with other law enforcement agents and others, and my review of documents, I understand that, on or about April 4, 2016, around the time of his reassignment to another branch within the CIA Group, many of SCHULTE's administrator privileges on the LAN were revoked, and he was no longer permitted to serve as a Systems Administrator in the CIA Group's LAN.

a. At the same time, on or about April 4, 2016, SCHULTE's computer access to a specific developmental project ("Project-1") was also revoked. Until his reassignment, SCHULTE had been the CIA Group employee with principal responsibility for Project-1.

b. Upon that transfer, principal responsibility for Project-1 was transferred to another CIA Group employee, who received computer access to Project-1.⁶

c. I know from my review of publicly available material on the Internet, including WikiLeaks.org, that Project-1 was one of a small group of CIA projects and capabilities that WikiLeaks highlighted explicitly by name in its March 7, 2017 press release that accompanied the online publication of the Classified Information.

15. Based on my conversations with other law enforcement agents and others, and my review of documents, I understand that, less than two weeks later, on or about April 11, 2016, SCHULTE unilaterally, and without authorization, logged onto the CIA Group's LAN and reinstated his own administrator privileges.

a. On or about April 14, 2016, CIA Group management discovered that

⁶ SCHULTE retained read-only access to Project-1 (but not the ability to alter the code) and the ability to copy the computer code associated with it in order to support another project for which he had responsibility.

SCHULTE had personally re-instituted his administrator privileges without permission.

b. On or about April 18, 2016, SCHULTE received notice regarding CIA policies against personnel restoring their own access to privileges or computer networks after those accesses have been revoked. SCHULTE signed an acknowledgment that he understood that “individuals are not permitted to personally attempt and/or renew their previous authorizations [including administrator privileges] to any particular [computer] system.” That notice further instructed SCHULTE: “do not attempt to restore or provide yourself administrative rights to any project and/or system for which they have been removed.”

c. A little more than one month later, on May 26, 2016, and notwithstanding the warnings described above, SCHULTE made an official request that he again be given full access to Project-1. Before receiving a response to that request, SCHULTE requested access from another employee who, apparently without proper vetting, granted SCHULTE the requested full access to Project-1.

i. On the same day, SCHULTE used that newly obtained access to, unilaterally and without authorization, revoke the computer access permissions of all other CIA Group employees to work on Project-1.

ii. Once this conduct was discovered, SCHULTE was issued a letter of warning that stated, “You were aware of the policy for access and your management’s lack of support for you to retain administrative privileges, but nonetheless you took steps to deliberately violate that policy and gain those privileges.” It continued by warning SCHULTE that any future violations would result in “further administrative action of a more severe nature.”

iii. After receiving the letter of warning, SCHULTE disagreed with some of its conclusions and consequently refused to sign the form.

16. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that the unauthorized duplication, retention and removal of the Classified Information from the CIA Group's computer network, and its placement on the publicly available Internet, exceeds the authorized access to those government-owned and controlled computer networks of any user. *See* 18 U.S.C. § 1030.

G. Internal CIA Investigation of SCHULTE and a CIA Colleague

17. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that, in or around March 2016, SCHULTE came to the attention of CIA security after SCHULTE alleged that another CIA Group co-worker had made a threat against him. SCHULTE expressed deep unhappiness about the way that CIA responded to the alleged threat. He threatened legal action against the CIA for its handling of the situation, and repeatedly stated that he felt that he was being punished by CIA management for reporting the alleged threat incident. SCHULTE informed CIA security that, if "forced into a corner" he would proceed with a lawsuit against the CIA. He also repeatedly threatened that he or his lawyer would go to the media. In addition, CIA security learned that SCHULTE had removed an internal CIA document from CIA facilities that regarded his complaints to the CIA concerning its handling of the alleged threat, despite being told multiple times by CIA security officials not to do so.

18. In approximately August 2016, as part of a standard background reinvestigation of SCHULTE for purposes of renewing his security clearances, the CIA conducted interviews of multiple CIA Group colleagues. Among other things:

a. Some (but not all) colleagues independently reported that SCHULTE's demeanor with his management and colleagues, and his commitment to his work, changed markedly for the worse in or around February 2016.

b. Multiple colleagues stated that SCHULTE had indicated that he felt aggrieved by the CIA in a number of respects. Some also reported that they believed SCHULTE to be untrustworthy and potentially subject to outside coercion. (Other colleagues made no such report and, indeed affirmatively reported that they believed that SCHULTE was, in fact, trustworthy.)

c. Some (but not all) colleagues also reported that SCHULTE's security practices were lax, and that SCHULTE tended not to abide by security guidelines he deemed inconvenient—particularly guidelines concerning when and what kinds of media or data (such as external drives) could be connected or uploaded to CIA computer systems.⁷

H. SCHULTE's November 2016 Resignation from the CIA

19. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that, in connection with and preceding SCHULTE's November 2016 resignation from the CIA, he sent the following communications, among others:

a. Approximately one month prior to his resignation, on October 12, 2016, SCHULTE, using his CIA email account, sent an email to another CIA Group employee at that employee's official email account. The subject line of the email stated, "ROUGH DRAFT of Resignation Letter *EYES ONLY*." The email contained a letter entitled "Letter of Resignation 10/12/16" and addressed to "To whomever it may concern" ("Draft Resignation Letter"). I know from reviewing the Draft Resignation Letter, which spanned approximately three single-spaced pages, the following:

⁷ External drives can be connected to computers and files in order to allow users to move files from the computers onto the portable external drives.

i. SCHULTE began the letter by stating, in substance and in part, that he had “always been a patriot” and would “obviously continue to support and defend this country until the day that I die,” but that “from this day forward” he would “no longer do so as a public servant.”

ii. SCHULTE claimed that he believed that the CIA Group management had unfairly “veiled” CIA leadership from various of SCHULTE’s previously expressed concerns, including concerns about the network security of the CIA Group’s LAN. SCHULTE continued: “That ends now. From this moment forward you can no longer claim ignorance; you can no longer pretend that you were not involved.”

iii. SCHULTE explained that he was resigning from the CIA because CIA Group management had, among other things, “ignored” issues he had raised about “security concerns” and had attempted to “conceal these practices from senior leadership,” including that the CIA Group’s LAN was “incredibly vulnerable” to the theft of sensitive data. He claimed that one named CIA Group manager had ignored his security concerns and “later attempt[ed] to evade responsibility and blame the decentralized and insecure [CIA Group computing] environment entirely on me.”⁸

iv. Specifically, SCHULTE wrote that inadequate CIA security measures had “left [the CIA Group’s LAN] open and easy for anyone to gain access and easily download [from the LAN] and upload [sensitive CIA Group computer code] in its entirety to the [public] internet.”

b. It appears that SCHULTE did not, in fact, submit the Draft Resignation

⁸ SCHULTE went on to describe other complaints he had about managers at the CIA. Among other things, SCHULTE described his complaints about the way in which CIA Group management had handled various personnel and disciplinary issues (*see supra* at Part II.G.16).

Letter.

c. On his last day with the CIA (November 10, 2016), SCHULTE did, however, send an internal email to the CIA Office of the Inspector General (OIG) advising that office that he had been in contact with the United States House of Representatives' Permanent Select Committee on Intelligence regarding his complaints about the CIA ("OIG Email").

i. In the OIG Email, which SCHULTE labeled "Unclassified," SCHULTE raised many of the same complaints included in the draft "Letter of Resignation 10/12/16," described above, including the CIA's treatment of him and its failure to address the "security concerns" he had repeatedly raised in the past.

ii. Shortly thereafter, CIA security learned that one of SCHULTE's colleagues had witnessed SCHULTE printing the OIG Email, placing it in a folder, and exiting the CIA Component facility where SCHULTE worked.

iii. Notwithstanding SCHULTE's labeling of the email as "Unclassified," the CIA subsequently determined that the OIG Email which SCHULTE removed from the CIA without authorization did, in fact, contain classified information.

I. SCHULTE's Recent Inquiries About the Status of the Investigation

20. Based on my conversations with other law enforcement agents and others, and my review of documents, I understand that, since the March 7, 2017 publication of the Classified Information on WikiLeaks, SCHULTE has repeatedly initiated contact, via telephone and text messages, with multiple of his former CIA Group colleagues. Those colleagues have reported that contact to government and law enforcement officials.

a. In those communications with his former colleagues, SCHULTE has repeatedly asked about the status of the investigation into the disclosure of the Classified Information.

b. SCHULTE has requested more details on the information that was disclosed.

c. SCHULTE has inquired of his interlocutors' personal opinions regarding who, within the CIA Group, each believes is responsible for the disclosure of the Classified Information. SCHULTE has also asked what other former CIA Group colleagues are saying about the disclosure.

d. SCHULTE has repeatedly denied any involvement in the disclosure of the Classified Information.

e. SCHULTE has indicated the he believes that he is a suspect in the investigation of the leak of Classified Information.

f. I am not aware of any other former CIA employee who has initiated any contact with former colleagues regarding the disclosure of the Classified Information.

J. SCHULTE' s Planned Travel

21. Based on my conversations with other law enforcement agents and others, and my review of documents, including information provided by the Department of Homeland Security, I understand that SCHULTE has booked an international flight departing in four days—Thursday, March 16, 2017. (Return travel to the United States is booked for a few days later.) The aforementioned records and conversations reflect that this is only SCHULTE's second trip reflected in in DHS records outside the United States.

K. Probable Cause Justifying Search of the Subject Premises

22. Thus, based on the above, I submit that there is probable cause to believe that SCHULTE has committed by the Subject Offenses by stealing a substantial amount of classified information from the CIA and has transmitting that information to individuals not authorized to receive it, thereby endangering the nation's national security. Based on my training and

experience, I know that individuals who are involved in the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials use computers and other electronic devices in furtherance of their criminal activities. Based on my training and experience, I also know that individuals typically keep their computers and other electronic devices in their homes.

23. Based on my participation in this investigation, I believe that SCHULTE resides at the Subject Premises. Among other things, I have reviewed records provided by SCHULTE's employer in New York City, which indicate that SCHULTE resides at the Subject Premises. I have also reviewed SCHULTE's credit card records, which reflect that SCHULTE resides at the Subject Premises. I have also spoken with other law enforcement officers who have observed SCHULTE enter and exit the Building on several occasions since on or about March 8, 2017. Those law enforcement officers have also told me that the Building has an electronic directory that lists SCHULTE's name as the individual residing in the Subject Premises.

L. Probable Cause Justifying Search of ESI

24. As noted above, individuals who engage in the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials often use computers and other electronic devices to store documents and records relating to their illegal activity. Individuals engaged in these activities use electronic devices to, among other things, store copies of classified documents or materials; engage in email correspondence relating to their illegal activity; store contact information of co-conspirators, including telephone numbers, email addresses, and identifiers for instant messaging and social medial accounts; and/or store records of illegal transactions involving classified documents.

25. Individuals who engage in the criminal activity described herein, in the event that they change computers, will often back up or transfer files from their old computers' hard drives to that of their new computers, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity. In addition, individuals who engage in such criminal activity will often also store or transfer files on electronic storage media other than computer hard drives, including thumb drives, flash memory cards, CD-ROMs, or portable hard drives to, for example, facilitate the use of the information or to transfer it to co-conspirators in support of the criminal scheme.

26. Individuals who engage in criminal activity involving computers and electronic devices also often maintain physical evidence of their criminal activity, including, among other things, printouts of documents and records that are also stored electronically, as described above, or handwritten notes of the same, for example as a backup in case of a failure of the electronic media on which they were stored or to facilitate use of the data.

27. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files can be stored on a hard drive for years at little or no cost. Even when such files have been deleted, they can often be recovered, depending on how the hard drive has subsequently been used, months or years later with forensics tools. Specifically, when a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Deleted files, or remnants of deleted files, may accordingly reside in "slack space" (space that is not being used for storage of a file) for long periods of time before they are overwritten. In addition, a computer's operating system may keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via

the Internet are generally automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve from a hard drive or other electronic storage media depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits.

28. Based on the foregoing, I respectfully submit that there is probable cause to believe that SCHULTE is committing or has committed the Subject Offenses, and that evidence of this criminal activity is likely to be found in the Subject Premises and on computers and electronic media found in the Subject Premises.

III. Items to Be Seized

29. Closed or Locked Containers. Based on my training, experience, participation in this and other investigations, I know that individuals who participate in criminal activities routinely secrete and store books, records, documents, currency and other items of the sort described in Attachment A in secure locations like safety deposit boxes, suitcases, safes, key-lock strong boxes, and other types of locked or closed containers in an effort to prevent the discovery or theft of said items. The requested warrant and search procedure includes a search of any closed containers on the Subject Premises, including cabinets, vehicles, doors to rooms, sheds, outbuildings, and other appurtenances located on or within the Subject Premises whether they are locked or unlocked.

30. Electronic Devices. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the requested warrants would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. Based upon my training and experience and information related to me by agents and others involved in the forensic

examination of computers, I know that computer data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, thumb drives, magnetic tapes and memory chips. I also know that during the search of the Subject Premises it may not be possible to fully search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process, which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.

b. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the Subject Premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 160 gigabytes (GB) of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 80 million pages of data, which, if printed out, would result in a stack of paper over four miles high.

c. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files;

however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

31. In light of these concerns, I hereby request the Court’s permission to copy at the Subject Premises information stored on computer hardware (and associated peripherals) that may contain some or all of the evidence described in Attachment A hereto, and to conduct an off-site search of such copies for the evidence described, using the general procedures described in Attachment A. However, to the extent law enforcement is unable to copy electronic devices at the Subject Premises, I hereby request the Court’s permission to seize those devices and search them off-site.

IV. Procedures for Searching ESI

A. Execution of Warrant for ESI

32. Federal Rule of Criminal Procedure 41(e)(2)(B) provides that a warrant to search for and seize property “may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information . . . for later review.” Consistent with Rule 41, this application requests authorization to search and/or seize any computer devices and storage media and transport them to an appropriate law enforcement facility for review. This is typically necessary for a number of reasons:

- First, the volume of data on computer devices and storage media is often impractical for law enforcement personnel to review in its entirety at the search location.
- Second, because computer data is particularly vulnerable to inadvertent or intentional modification or destruction, computer devices are ideally examined in a controlled environment, such as a law enforcement laboratory, where trained personnel, using specialized software, can make a forensic copy of the storage media that can be subsequently reviewed in a manner that does not change the underlying data.
- Third, there are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized personnel and equipment potentially required to safely access the underlying computer data.
- Fourth, many factors can complicate and prolong recovery of data from a computer device, including the increasingly common use of passwords, encryption, or other features or configurations designed to protect or conceal data on the computer, which often take considerable time and resources for forensic personnel to detect and resolve.

B. Review of ESI

33. Following the search of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained therein for information responsive to the warrant.

34. In conducting this review, law enforcement personnel may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- conducting a file-by-file review by “opening” or reading the first few “pages” of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);
- “scanning” storage areas to discover and possibly recover recently deleted data or deliberately hidden files; and
- performing electronic keyword searches through all electronic storage areas to determine the existence and location of search terms related to the subject matter of the investigation. (Keyword searches alone are typically inadequate to detect all information subject to seizure. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.)

35. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement personnel may need to conduct a complete review of all the ESI from searched devices or storage media to evaluate its contents and to locate all data responsive to the warrant.

C. Return of ESI

36. If the Government seizes any electronic devices, later determines that the electronic devices are no longer necessary to retrieve and preserve the data, and the items are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return these items, upon request. Computer data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the

offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the Subject Offenses.

V. Execution of the Search Warrant: Necessity of Covert Search and Delayed Notification

37. I respectfully request that the search warrant permit law enforcement agents to execute the search at any time in the day or night. I also respectfully request that the search warrant permit law enforcement agents to execute the search warrant covertly without advance or contemporaneous notice of the execution of the warrant, or if they deem covert execution impracticable to execute the search warrant overtly without further order of the Court. Law enforcement agents will provide notice of the execution of the warrant, if it is executed covertly, within seven days of execution unless there is a new showing, made to the Court, that delayed notice is appropriate. If the warrant is executed overtly, notice will be provided at or as soon as practicable after the execution.

a. As described in greater detail above and below, there is probable cause to believe that SCHULTE has stolen a substantial amount of classified information and transmitted that information to those not authorized to receive it, thereby endangering the nation's national security.

b. SCHULTE likely engaged in these activities by using sophisticated computer skills to exfiltrate a substantial amount of data onto a removable drive and then covertly removed that drive from the CIA.

c. If SCHULTE is provided advance or contemporaneous notice of the execution of this search warrant, it may allow him to destroy evidence of his crimes on electronic devices by, for example, deleting drives or activating encryption programs that would make his devices virtually impossible to access.

d. Moreover, law enforcement agents will likely need some time to review and analyze any electronic devices identified at the Subject Premises. If SCHULTE is provided advance or contemporaneous notice of the search of the Subject Premises, he may be able to destroy evidence that can be developed based on the search of electronic devices.

38. Pursuant to Title 18, United States Code, Section 3103a(b)(1), delayed notification may be provided for a search warrant obtained pursuant to Rule 41 of the Federal Rules of Criminal Procedure if “the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result.” Delayed notification pursuant to this provision may only be provided for a reasonable period not to exceed 30 days, although it may be extended by the court for good cause shown, pursuant to Title 18, United States Code, Sections 3103a(b)(3) and 3103(c). A delayed notice warrant obtained pursuant to this provision prohibits “the seizure of tangible property, any wire electronic communication (as defined in section 2510), or, except as expressly provided in chapter 121, any stored wire or electronic information, *except where the court finds reasonable necessity for the seizure.*” Title 18, United States Code, Section 3103(b)(2) (emphasis added).

39. The investigation of the Subject Offenses and SCHULTE is on-going, and remains extremely sensitive. The FBI is continuing to review an enormous volume of electronic evidence, much of which remains highly classified and extremely sensitive. In addition, based on *inter alia* the statements in WikiLeaks March 7, 2017 press release accompanying the Classified Information, it appears at least possible that additional CIA information may have been stolen and provided to WikiLeaks or others not authorized to receive it. Accordingly, ensuring that the investigation remains covert for as long as possible is at its zenith. Public disclosure of the search prematurely could cause evidence to be destroyed or additional information to be hastily released

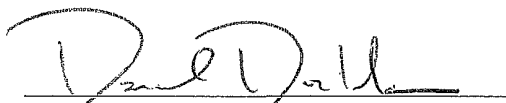
onto the Internet. In that context, I know, based on my review of the WikiLeaks press release, that they claimed to have refrained from publishing additional information they purport to possess such as “‘armed’ cyberweapons,” which I understand based on my training, experience and involvement in this investigation to mean the specific computer code they claim could actually be used to perpetrate a cyber-attack or penetration). They also claim to have “anonymi[zed] some identifying information,” which I understand, based on my training, experience, and involvement in this investigation, to include the names of covert CIA operatives and possibly covert United States Government locations. Finally, because SCHULTE has booked an overseas trip for this Thursday, it is critical that, to the extent possible, the search be conducted in such a way as to minimize the possibility that it causes him to flee or to destroy evidence. In light of the foregoing, it is reasonably necessary to conduct the search requested herein covertly.

40. Consistent with Title 18, United States Code, Section 3103a(b)(2), this application requests that any notice otherwise required for the seizure and search of information be delayed for a period of 30 days in light of the reasonable necessity – comprising both the investigatory aims and mitigating goals of this investigation – for such a delay.

VI. Conclusion and Ancillary Provisions

41. Based on the foregoing, I respectfully request the court to issue a warrant to search and seize the items and information specified in Attachment A to this Affidavit and to the Search and Seizure Warrant.

42. In light of the confidential nature of the continuing investigation, I respectfully request that this Affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise.


JEFF D. DONALDSON
Special Agent
Federal Bureau of Investigation

Sworn to before me on
this 13th day of March 2017


S/Barbara Moses

THE HONORABLE BARBARA MOSES
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK

Attachment A

I. Premises to be Searched—Subject Premises

The premises to be searched (the “Subject Premises”) is described as follows, and includes all locked and closed containers found therein:

The Subject Premises is particularly described as apartment 8C in a building located at 200 East 39th Street, New York, New York 10016 (the “Building”). The Building is located near the corner of 39th Street and Third Avenue. The Building is nineteen stories high and contains approximately ninety-one apartment units. The Subject Premises is a one-bedroom apartment located on the eighth floor of the Building, and it is clearly identifiable as apartment 8C from the outside of the Subject Premises.

II. Execution of the Warrant

Law enforcement agents are permitted to execute the search warrant at any time in the day or night, and further to execute the search warrant covertly without advance or contemporaneous notice of the execution of the search warrant. Law enforcement agents will provide notice of the execution of the warrant within seven days of execution unless there is a new showing, made to the Court, that delayed notice is appropriate.

III. Items to Be Searched and Seized

A. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be searched and/or seized from the Subject Premises include the following evidence, fruits, and instrumentalities of: (i) the unauthorized possession and, *inter alia*, the communication of national defense information to someone not entitled to receive it, in violation of Title 18, United States Code, Section 793(d); (ii) the unlawful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); (iii) exceeding authorized access to a computer in order to obtain national defense information with reason to believe that information could be used to the injury of the United States and the advantage of a foreign nation and willfully transmitting that information to a person not entitled to receive it, in violation of Title

18, United States Code, Section 1030(a)(1); and (iv) intentionally exceeding authorized access and thereby obtaining information from a department or agency of the United States, in violation of Title 18, United States Code, Section 1030(a)(2)(B) (collectively, the “Subject Offenses”):

1. Evidence concerning occupancy or ownership of the Subject Premises, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys.

2. Evidence concerning the identity or location of, and communications with, any co-conspirators.

3. Any and all notes, documents, records, correspondence, or materials, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, and handwritten notes), pertaining to the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials.

4. Electronic devices (including but not limited to computers, tablets, smartphones, and cellular telephones) and storage media used in furtherance of the Subject Offenses, containing evidence of the Subject Offenses, or containing evidence authorized for seizure in paragraphs 1, 2 and 3 above. The term “storage media” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

5. Electronic forensic evidence relating to the Subject Offenses, including for any electronic device or storage media whose search and/or seizure is authorized by this warrant as described above in paragraph 4 (hereinafter, “Computers”¹), including:

- a. evidence of the times the Computers were used in furtherance of the Subject Offenses;
- b. passwords, encryption keys, and other access devices that may be necessary to access the Computers;
- c. documentation and manuals that may be necessary to access the Computers or to conduct a forensic examination of the Computers;
- d. evidence of software that would allow others to control the Computers, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- e. evidence indicating how and when the Computers were accessed or used in furtherance of the Subject Offenses;
- f. evidence indicating the Computers’ user’s/users’ state of mind as it relates to the Subject Offenses;
- g. evidence of the attachment to the Computers of other storage devices or similar containers for electronic evidence in furtherance of the Subject Offenses;

¹ The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

- h. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Computers;
- i. records of or information about Internet Protocol addresses used by the Computers;
- j. records of or information about the Computers' Internet activity in furtherance of the Subject Offenses, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

6. If law enforcement personnel seize the computer(s) or other electronic device(s), the personnel will search the computer and/or device(s) within a reasonable amount of time, not to exceed 60 days from the date of execution of the warrant. If, after such a search has been conducted, it is determined that a computer or device contains any data listed in paragraphs 1 through 3, the Government will retain the computer or device. If it is determined that the computer(s) or device(s) are no longer necessary to retrieve and preserve the data, and the items are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(b), such materials and/or equipment will be returned within a reasonable time. In any event, such materials and/or equipment shall be returned no later than 60 days from the execution of this warrant, unless further application is made to the Court.

B. Search and Seizure of Electronically Stored Information

The items to be searched and seized from the Subject Premises also include any computer devices and storage media that may contain any electronically stored information falling within the categories set forth in Section III.A of this Attachment above, including, but not limited to,

desktop and laptop computers, disk drives, modems, thumb drives, personal digital assistants, smart phones, digital cameras, and scanners. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

The items to be searched and seized from the Subject Premises also include:

1. Any items or records needed to access the data stored on any seized or copied computer devices or storage media, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.
2. Any items or records that may facilitate a forensic examination of the computer devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.
3. Any evidence concerning the persons with access to, control over, or ownership of the seized or copied computer devices or storage media.

C. Review of ESI

Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques, including but not limited to:

- surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few "pages" of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files;
- scanning storage areas for deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- making reasonable efforts to utilize computer search methodology to search only for files, documents, or other electronically stored information within the categories identified in Sections I.A and I.B of this Attachment.

Exhibit C
Subject Devices Seized from Schulte Residence

Item #	Description
1B56	Rack server, no serial number
1B55	Black tower computer, no serial number
1B54	One bag containing seven CD/DVDs
1B53	One bag containing twenty-seven CD/DVDs
1B52	One bag containing twenty-eight CD/DVDs
1B51	One bag containing twenty-nine CD/DVDs
1B50	One bag containing fifteen CD/DVDs
1B49	One bag containing 9 floppy disks, and five CD/DVDs
1B48	One ATT Sim Card
1B47	One 16GB Micro SD
1B46	One 8 GB SanDisk Micro SD
1B45	One UFCU 128MB Thumb Drive
1B44	One Sans Thumb Drive
1B43	One SanDisk 1GB Thumb Drive
1B42	One PNY 1GB Thumb Drive
1B41	One OSR Thumb Drive
1B40	One SanDisk USB Thumbdrive 16GB
1B39	One TP-Link Network USB
1B38	One Garmin NUVI S/N: 1C2041768
1B37	One HTC Phone S/N: HT806G001901
1B36	One MS ZUHE Mp3 Player S/N: 014195164210
1B35	One Olympus Camera JOH244018
1B34	One HTC Cell Phone S/N: HTO68P900155
1B33	One Samsung Phone Model: SPHL710
1B32	One Western Digital 1 TB Hard Disk Drive ("HDD") S/N: WCAW32653861
1B31	One 640 GB Western Digital HDD S/N: WCASY0416918
1B30	One 160GB Western Digital HDD S/N: WMAU2U189169
1B29	One Samsung 1 TB HDD S/N: 52AEJ18Z408962
1B28	One Samsung 1 TB HDD S/N: S2AEJ18Z4408961
1B27	One Samsung 1 TB HDD S/N: S2AEJ18Z408963
1B26	One Western Digital 1 TB Hard Drive ("HD") S/N: WCAU45276871
1B25	One Western Digital 1 TB HDD S/N: WCAU42139599
1B24	One Western Digital 1 TB HDD S/N: WCAW32328401
1B23	One Western Digital 1 TB HDD S/N: WCAU45355046
1B22	One Kingston Hyper X Solid State Drive ("SSD")
1B21	One 120GB Samsung SSD S19HNSAD5517655
1B20	One black server tower, no serial number
1B19	One Samsung Phone Model SM-J320P
1B18	One Kindle
1B17	One Samsung tablet S/N: R52H60LF5RY
1B16	One Kindle
1B15	One Xbox1 S/N: 149212254048
1B14	One Xbox 360s S/N: 033320322443

JAS_000208

JAS_027222

Exhibit C
Subject Devices Seized from Schulte Residence

FBI Item #	Description
1B13	One SanDisk MP3 Player
1B12	One SanDisk MP3 Player
1B10	One SanDisk Thumbdrive
1B9	One black server tower

JAS_000209

JAS_027223

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF:)
Electronic Devices Previously Seized from the)
Premises of 200 East 39th Street, Apartment 8C,)
New York, NY 10016)

UNDER SEAL

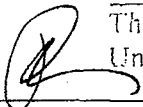
Case No. 1:17-SW- 199

ORDER TO SEAL

The UNITED STATES, pursuant to Local Rule 49(B) of the Local Criminal Rules for the United States District Court for the Eastern District of Virginia, having moved to seal the search warrant, the application for search warrant, the affidavit in support of the search warrant, the Motion to Seal, and proposed Order in this matter; and

The COURT, having considered the government's submissions, including the facts presented by the government to justify sealing; having found that revealing the material sought to be sealed would jeopardize an ongoing criminal investigation; having considered the available alternatives that are less drastic than sealing, and finding none would suffice to protect the government's legitimate interest in concluding the investigation; and having found that this legitimate government interest outweighs at this time any interest in the disclosure of the material; it is hereby

ORDERED, ADJUDGED, and DECREED that, the search warrant, application for search warrant, affidavit in support of the search warrant, Motion to Seal, and this Order be sealed until further Order of the Court.

/s/
Theresa Carroll Buchanan
United States Magistrate Judge

Theresa C. Buchanan
United States Magistrate Judge

Date: 4/14/17
Alexandria, Virginia

JAS_000210

JAS_027224

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

APR 14 2017

IN THE MATTER OF THE SEARCH OF:) UNDER SEAL
Electronic Devices Previously Seized from the)
Premises of 200 East 39th Street, Apartment 8C,) Case No. 1:17-SW- 199
New York, NY 10016.)

**GOVERNMENT'S MOTION TO SEAL SEARCH WARRANT
PURSUANT TO LOCAL RULE 49(B)**

The United States of America, by and through undersigned counsel, upon the return of its executed search warrant,¹ and pursuant to Local Rule 49(B) of the Local Criminal Rules for the United States District Court for the Eastern District of Virginia, now asks for an Order to Seal the search warrant, application for the search warrant and the affidavit in support of the search warrant, together with this Motion to Seal and proposed Order, until the United States makes a motion to unseal the search warrant and affidavit.

I. REASONS FOR SEALING (See Local Rule 49(B)(1))

1. At the present time, Special Agents of the Federal Bureau of Investigation (FBI) are conducting an investigation into: (i) violations of Title 18, United States Code, Section 2252 (possession, transportation, receipt, distribution, production, and reproduction of sexually explicit material relating to children) and Title 18, United States Code, Section 2252A (activities relating to material constituting or containing child pornography); and (ii) violations of Title 17, United States Code, Section 506 and Title 18, United States Code, Section 2319 (criminal infringement of a copyright).

¹ Pursuant to Local Rule 49(B), "[n]o separate motion to seal is necessary to seal a search warrant *from the time of issuance to the time the executed warrant is returned.*" (Emphasis added.) This is because, as Rule 49(B) additionally mandates, "[u]ntil an executed search warrant is returned, search warrants and related papers are not filed with the Clerk."

JAS_000211

JAS_027225

2. Premature disclosure of the specific details of this ongoing investigation (as reflected, for example, in the affidavit in support of search warrant) would jeopardize this continuing criminal investigation and may lead to the destruction of additional evidence in other locations. Thus, a sealing order is necessary to avoid hindering the ongoing investigation in this matter.

3. The United States has considered alternatives less drastic than sealing, including, for example, the possibility of redactions, and has determined that none would suffice to protect this investigation.

II. THE GOVERNING LAW (See Local Rule 49(B)(2))

4. It is generally recognized that the public has a common law right of access, but not a First Amendment right of access, to judicial documents, including documents associated with *ex parte* proceedings such as search warrant affidavits. Media General Operations, Inc. v. Buchanan, 417 F.3d 424, 429 (4th Cir. 2005); In re Washington Post Company v. Hughes, 923 F.2d 324, 326 (4th Cir. 1991). “But the right of access is qualified, and a judicial officer may deny access to search warrant documents if sealing is ‘essential to preserve higher values’ and ‘narrowly tailored to serve that interest.’” Media General Operations, 417 F.3d at 429 (citations omitted); see also In re Knight Pub. Co., 743 F.2d 231, 235 (4th Cir. 1984) (“[t]he trial court has supervisory power over its own records and may, in its discretion, seal documents if the public’s right of access is outweighed by competing interests”). Sealing search warrants and their accompanying affidavits and application is within the discretionary powers of a judicial officer where, among other things, an “‘affidavit contain[s] sensitive details of an ongoing investigation’ and it is ‘clear and apparent from the affidavits that any disclosure of the

information there would hamper' th[e] ongoing investigation." Media General Operations, 417 F.3d at 430 (citations omitted); see also In re Search Warrant for Matter of Eye Care Physicians of America, 100 F.3d 514, 518 (7th Cir. 1996).

5. Before a district court generally may seal judicial records or documents, it must (a) provide public notice of the request to seal and allow interested parties a reasonable opportunity to object, (b) consider less drastic alternatives to sealing the documents, and (c) provide specific reasons and factual findings supporting its decision to seal the documents and for rejecting the alternatives. Ashcraft v. Conoco, Inc., 218 F.3d 288, 302 (4th Cir. 2000).

6. However, regarding the notice requirement in the specific context of a search warrant, the Fourth Circuit has cautioned that "the opportunity to object" cannot "arise prior to the entry of a sealing order when a search warrant has not been executed." Media General Operations, 417 F.3d at 429. "A rule to the contrary would endanger the lives of officers and agents and allow the subjects of the investigation to destroy or remove evidence before the execution of the search warrant." Id.; see also Franks v. Delaware, 438 U.S. 154, 169 (1978). Accordingly, in the context of search warrants, "the notice requirement is fulfilled by docketing 'the order sealing the documents,' which gives interested parties the opportunity to object after the execution of the search warrants." Media General Operations, 417 F.3d at 430 (quoting Baltimore Sun Co. v. Goetz, 886 F.2d 60, 65 (4th Cir. 1989)); see also Local Rule 49(B) ("Until an executed search warrant is returned, search warrants and related papers are not filed with the Clerk.").

7. As to the requirement of a court's consideration of alternatives, the Fourth Circuit counsels that, "[i]f a judicial officer determines that full public access is not appropriate, she 'must consider alternatives to sealing the documents,' which may include giving the public

access to some of the documents or releasing a redacted version of the documents that are the subject to the government's motion to seal.” Media General Operations, 417 F.3d at 429 (quoting Goetz, 886 F.2d at 66).

8. Finally, regarding the requirement of specific findings, the Fourth Circuit's precedents state that, “in entering a sealing order, a ‘judicial officer may explicitly adopt the facts that the government presents to justify sealing when the evidence appears creditable,’” Media General Operations, 417 F.3d at 429 (quoting Goetz, 886 F.2d at 65), so long as the ultimate “decision to seal the papers” is “made by the judicial officer,” Goetz, 886 F.2d at 65. “Moreover, if appropriate, the government’s submission and the [judicial] officer’s reason for sealing the documents can be filed under seal.” Goetz, 886 F.2d at 65; see also In re Washington Post Co., 807 F.2d 383, 391 (4th Cir. 1986) (“if the court concludes that a denial of public access is warranted, the court may file its statement of the reasons for its decision under seal”).

III. PERIOD OF TIME GOVERNMENT SEEKS TO HAVE MATTER REMAIN UNDER SEAL (See Local Rule 49(B)(3))

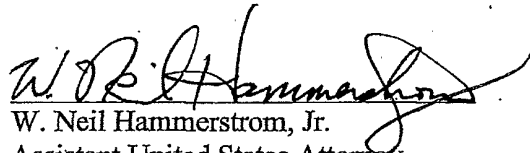
9. Pursuant to Local Rule 49(B)(3), the search warrant and the affidavit will remain sealed until the need to maintain the confidentiality of the search warrant application and the related investigation expires, after which time the United States will move to unseal the search warrant and affidavit.

WHEREFORE, the United States respectfully requests that the search warrant, application for search warrant, affidavit in support of the search warrant, and this Motion to Seal and proposed Order be sealed until further Order of the Court.

Respectfully submitted,

Dana J. Boente
United States Attorney

By:


W. Neil Hammerstrom, Jr.
Assistant United States Attorney

AO 93 (Rev. 12/09) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

In the Matter of the Search of
 (Briefly describe the property to be searched
 or identify the person by name and address)
 Electronic Devices Previously Seized from the
 Premises of 200 East 39th Street, Apartment 8C,
 New York, NY 10016

Case No. 1:17-SW- 199

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Virginia
 (identify the person or describe the property to be searched and give its location):

Electronic devices located at a U.S. Government facility in Herndon, Virginia

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

SEE ATTACHMENT A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before April 28, 2017

(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m. ☒ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge Theresa C. Buchanan

(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) ☐ for days (not to exceed 30).

☐ until, the facts justifying, the later specific date of

Theresa C. Buchanan

United States Magistrate Judge

Date and time issued: 4/14/17 2:20p

Judge's signature

City and state: Alexandria, Virginia

Theresa C. Buchanan, United States Magistrate Judge

Printed name and title

JAS_000216

JAS_027230

Attachment A

I. Devices to be Searched—Subject Devices

The devices to be searched (the “Subject Devices”) include any and all electronic devices seized pursuant to a search warrant executed on or about March 15, 2017 at the premises described as apartment 8C in a building located at 200 East 39th Street, New York, New York 10016.

II. The Search of the Subject Devices

A. Evidence, Fruits, and Instrumentalities of the Child Pornography Offenses

The Subject Devices may be searched for the following evidence, fruits, and/or instrumentalities of violations of Title 18, United States Code, Sections 2252 (activities relating to material constituting or containing child pornography) and 2252A (possession, transportation, receipt, distribution, production, and reproduction of sexually explicit material relating to children) (the “CP Offenses”):

- Evidence of computer programs used to access, transmit, or store information relating to the CP Offenses;
- Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from computer devices, storage media, and related electronic equipment;
- Evidence of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
- Motion pictures, films, videos, and other recordings of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
- Correspondence and records pertaining to violation of the CP Offenses including, but not limited to electronic mail, chat logs, electronic messages, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions involving any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
- Records or other items which evidence ownership, control, or use of, or access to computer devices, storage media, and related electronic equipment used to access, transmit, or store information relating to the CP Offenses, including but not limited to sales receipts, warranties, bills for internet access, registry entries, configuration files, saved usernames and passwords, user profiles, email contacts, and photographs.

- Information or correspondence pertaining to affiliation with any child exploitation bulletin boards, chat forums, or organizations;
- Any child pornography as defined by 18 U.S.C. § 2256(8);
- Any child erotica, defined as suggestive visual depictions of nude minors which do not constitute child pornography as defined by 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined by 18 U.S.C. § 2256(2);
- Notes, documents, records, invoices, or correspondence, in any format and medium, including, but not limited to, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);
- Names, and lists of names and addresses of individuals (including minors) related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);
- Mailing lists and/or supplier lists related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2); and
- Financial records, including credit card information, bills, and payment records related to related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

B. Evidence, Fruits, and Instrumentalities of the Copyright Offenses

The Subject Devices may also be searched for the following evidence, fruits, and/or instrumentalities of violations of violations of 17 U.S.C. § 506 and 18 U.S.C. § 2319 (criminal infringement of a copyright) (the “Copyright Offenses”):

- Evidence of computer programs used to transmit or store information relating to the Copyright Offenses;
- Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from computer devices, storage media, and related electronic equipment;

- Evidence of copyrighted works, including motion pictures, films, videos, other recordings, and documents relating to the Copyright Offenses;
- Correspondence and records pertaining to violation of the Copyright Offenses including, but not limited to electronic mail, chat logs, electronic messages, and records bearing on the transmission, receipt, and/or storage of copyrighted works;
- Records or other items which evidence ownership, control, or use of, or access to computer devices, storage media, and related electronic equipment used to transmit or store information relating to the Copyright Offenses, including but not limited to sales receipts, warranties, bills for internet access, registry entries, configuration files, saved usernames and passwords, user profiles, email contacts, and photographs.
- Any copyrighted works;
- Notes, documents, records, invoices, or correspondence, in any format and medium, including, but not limited to, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, related to the transmission, receipt, and/or storage of copyrighted works;
- Names, and lists of names and addresses of individuals (including minors) related to the transmission, receipt, and/or storage of copyrighted works;
- Mailing lists and/or supplier lists related to the transmission, receipt, and/or storage of copyrighted works; and
- Financial records, including credit card information, bills, and payment records related to the transmission, receipt, and/or storage of copyrighted works.

C. Review of ESI

In conducting a review of ESI on the Subject Devices, law enforcement personnel may use various techniques, including but not limited to:

- surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few "pages" of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files;
- scanning storage areas for deliberately hidden files;

- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- making reasonable efforts to utilize computer search methodology to search only for files, documents, or other electronically stored information within the categories identified in Section II.A of this Attachment.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Section II.A of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all ESI from the Subject Devices if necessary to evaluate its contents and to locate all data responsive to the warrant.

UNITED STATES DISTRICT COURT

for the
Southern District of New YorkIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

(1) Workstation 173 on 16th floor of Bloomberg L.P., 120 Park Ave. New York, NY 10017, as well as Any Closed Containers/Items Contained Therein; & (2) Samsung internal solid state drive, model no. MZ-HPU512T/0H1 & serial no. S1L5NYAG301784; see Attachment A

17 MAG 3418
Case No.

APPLICATION FOR A SEARCH AND SEIZURE WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

(1) Workstation 173 on 16th floor of Bloomberg L.P., 120 Park Ave. New York, NY 10017, as well as Any Closed Containers/Items Contained Therein; & (2) Samsung internal solid state drive, model no. MZ-HPU512T/0H1 & serial no. S1L5NYAG301784; see Attachment A.

located in the Southern District of New York, there is now concealed (identify the person or describe the property to be seized):

See Attached Affidavit and its Attachment A

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section(s)	Offense Description(s)
18 U.S.C. 793(d), 793(e), 1030(a)(1), 1030(a)(2)(B), 2252, 2252A, 2319; 17 U.S.C. 506.	Offenses relating to unauthorized possession and distribution of national defense information; child pornography; and copyright infringement.

The application is based on these facts:

See Attached Affidavit and its Attachment A

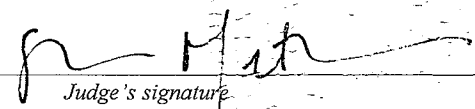
- ☒ Continued on the attached sheet.
- ☒ Delayed notice of 30 days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature
Special Agent Jeff D. Donaldson, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 05/05/2017

City and state: New York, NY


Judge's signature
Honorable Sarah Netburn
Printed name and title

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of the Application of the United States of America for a Search Warrant for the Premises Known and Described as (1) Workstation Number 173 on the 16th floor of Bloomberg L.P., located at 120 Park Avenue, New York, New York 10017, as well as Any Closed Containers/Items Contained Therein; and (2) a Samsung internal solid state drive with model number MZ-HPU512T/0H1 and serial number S1L5NYAG301784.

TO BE FILED UNDER SEAL

**Agent Affidavit in Support of
Application for Search Warrant**

SOUTHERN DISTRICT OF NEW YORK) ss.:

JEFF D. DONALDSON, being duly sworn, deposes and says:

I. Introduction

A. Affiant

1. I am a Special Agent of the Federal Bureau of Investigation (“FBI”) assigned to the New York Field Office, and have been employed by the FBI since 2010. I am currently assigned to a squad responsible for counterespionage matters and have worked in the field of counterintelligence from 2010 to present. In the course of my duties as a Special Agent, I am responsible for investigating offenses involving espionage and related violations of law, including unauthorized retention, gathering, transmitting or losing classified documents or materials; unauthorized removal and retention of classified documents or materials; illegally acting in the United States as a foreign agent; other national security offenses; and the making of false statements. As a result of my involvement in espionage investigations and investigations involving the unauthorized disclosure or retention of classified information, as well as my training in counterintelligence operations, I am familiar with the tactics, methods, and techniques of United States persons who possess, or have possessed, a United States Government security clearance and

who may choose to harm the United States by misusing their access to classified information. I am also familiar, though my training and experience with the use of computers in criminal activity and the forensic analysis of electronically stored information.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises specified below (the “Subject Premises”) for the items and information described in Attachment A. This Affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information (“ESI”). Because this Affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. The Subject Premises

3. The Subject Premises are particularly described as, collectively:

a. Workstation number 173 (“Workstation 173”) on the 16th floor of the offices of Bloomberg LP, located at 120 Park Avenue, New York, New York 10017, which is an office space within a tan commercial high-rise office building (the “Building”) located on the Northwest corner of Park Avenue and East 41st Street in Manhattan, as well as any closed containers or items contained therein or related thereto (“Subject Premises-1”), including but not limited to any servers that contain images or back-up copies of any electronic media (as defined herein) contained within or assigned to Workstation 173, or electronically generated logs of activity conducted within Workstation 173, to the extent such servers or electronically generated

logs are maintained by Bloomberg LP. The exterior of the Building has a glass entrance with the number “120” visible from the exterior.

b. A computer hard drive, which presently is in the possession, custody, and control of the FBI in the Southern District of New York, known and described as: a Samsung internal solid state drive with model number MZ-HPU512T/0H1 and serial number S1L5NYAG301784 (the “Subject Premises-2”) (collectively, with Subject Premises-1, the “Subject Premises”).

C. The Subject Offenses

4. For the reasons detailed below, I believe that there is probable cause that the Subject Premises contain evidence, fruits, and instrumentalities of: (i) the unauthorized possession and, *inter alia*, the communication of national defense information to someone not entitled to receive it, in violation of Title 18, United States Code, Section 793(d); the unlawful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); exceeding authorized access to a computer in order to obtain national defense information with reason to believe that information could be used to the injury of the United States and the advantage of a foreign nation and willfully transmitting that information to a person not entitled to receive it, in violation of Title 18, United States Code, Section 1030(a)(1); intentionally exceeding authorized access to a computer and thereby obtaining information from a department or agency of the United States, in violation of Title 18, United States Code, Section 1030(a)(2)(B) (collectively, the “National Security and Computer Crime Offenses”); (ii) violations of Title 18, United States Code, Section 2252 (possession, transportation, receipt, distribution, production, and reproduction of sexually explicit material relating to children) and Title 18, United States Code, Section 2252A (activities relating to material constituting or containing child pornography) (collectively, the “CP Offenses”); and (iii) violations of Title 17, United States Code, Section 506 and Title 18, United

States Code, Section 2319 (criminal infringement of a copyright) (the “Copyright Offenses,” and collectively with the National Security and Computer Crime Offenses as well as the CP Offenses, the “Subject Offenses”).

D. Terminology

5. The term “computer,” as used herein, is defined as set forth in 18 U.S.C. § 1030(e)(1).

6. The terms “records,” “documents,” and “materials” include all information recorded in any form, visual or oral, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical discs, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device), as well as the equipment needed to record such information (including but not limited to cameras and video recording and storage devices).

7. The term “child pornography” is defined in Title 18, United States Code, Section 2256(8), in pertinent part as “any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic,

mechanical, or other means, of sexually explicit conduct, where . . . the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct.”¹

8. The terms “minor,” “sexually explicit conduct” and “visual depiction” are defined as set forth in Title 18, United States Code, Section 2256.

II. Probable Cause and Request to Search

A. Probable Cause Relating to the National Security and Computer Crime Offenses

9. Based on my review of publicly available material on the Internet, including on the website wikileaks.org (“WikiLeaks”), I know that, on March 7, 2017, WikiLeaks published what it claimed were more than 8,000 documents and files that contained classified information (the “Classified Information”) belonging to the Central Intelligence Agency (“CIA”). In its press release accompanying the Classified Information, WikiLeaks further claimed that:

a. The public dissemination of the Classified Information was “the largest ever” unauthorized publication of classified CIA documents.

b. The Classified Information constituted the “first full part” of a series—thus indicating that there would be subsequent publications of additional sensitive CIA information.²

c. The “collection” obtained by WikiLeaks amounted to “more than several hundred million lines of code” and revealed the “entire hacking capacity” of the CIA, including various malware, viruses, and other tools used by the CIA.

¹ See also *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002) (analyzing constitutional validity of the definitions set forth in 18 U.S.C. § 2256(8)).

² On or about March 24, 2017, March 31, 2017, April 7, 2017, April 14, 2017, April 21, 2017, April 28, and May 5, 2017, WikiLeaks released additional batches of documents that it claimed were also obtained from the CIA.

hard drive. According to publicly available materials published by Microsoft, the “robocopy” function would allow a user “to mirror the contents of an entire folder hierarchy across local volumes or over a network. . . . Robocopy is a powerful tool, capable of moving, copying, and deleting files and folders faster than you can say ‘Whoops.’” In addition, the Robocopy command allows a user to copy an entire file storage directory sporadically, rather than all at one time. It does that by enabling the copying process to proceed in increments and re-start from where it left off, rather than requiring a user to start the copying process over again from the beginning.

d. On the following day, April 13, 2016, SCHULTE conducted Google Searches apparently designed to gather information about the speed of various portable, external computer hard drives, such as “thumb drives” and “flash drives,” which are computer memory storage devices that connect to a computer typically via a USB port, including searches for:

- i. “thumbdrive copy speed”;
- ii. “flash drive transfer rate”; and
- iii. “flash drive read speeds”

e. Later in the day on April 13, 2016, within minutes of conducting the Google Searches regarding portable hard drive speeds, SCHULTE also conducted another Google Search apparently designed to identify the most efficient way to copy units of computer data: “optimal reading chunk size c++”. I know, based on my training, experience and conversations with other law enforcement agents with technical expertise regarding computers, that:

i. Computers store, read and write data in units that are sometimes referred to as “blocks” or “chunks.” When data is copied, each block or chunk is separately read, copied and written from the original storage location to the destination storage location. These

10. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that:

a. The information that WikiLeaks claimed was classified CIA information—that is, the Classified Information—was at the time of its disclosure, in fact, classified CIA information.

b. Specifically, the Classified Information was created and maintained by one specific group within the CIA which is responsible for various computer engineering activities, including the development of computer code (the “CIA Group”). That CIA Group exists within a larger CIA component (the “CIA Component”). In March 2016, less than 200 employees were assigned to the CIA Group.

c. The Classified Information was maintained by the CIA Group on an isolated local-area computer network (the “LAN”).³ Only employees of the CIA Group had access to the LAN on which the Classified Information was stored.⁴

i. An isolated network, such as the CIA Group’s LAN, is a network-security structure by which the isolated network is physically separated (or “air-gapped”) from

³ In its press release announcing the publication of the Classified Information, WikiLeaks stated that the Classified Information originated from “an isolated, high-security network.”

⁴ Prior search warrant applications in connection with this investigation set forth that a preliminary analysis had concluded that the Classified Information was likely copied from a back-up server to which the same three systems administrators likely had access. The information that the Classified Information was likely recovered from an automated back-up file to which only systems administrators likely had access was first received by the FBI on or about March 22, 2017. As set forth herein, an investigation is ongoing as to whether the stolen data was in fact back-up data taken from the automated back-up. But, nevertheless, the current assessment remains that the copying of the data, regardless of the data’s original location, would likely have required systems administrator access of the type maintained by TARGET SUBJECT JOSHUA ADAM SCHULTE. Accordingly, we respectfully submit that the precise location from where the Classified Information was taken—whether from an automated back-up file or from a non-back-up computer file—does not affect the probable cause underlying the prior search warrant applications.

unsecured networks, such as the public Internet.

ii. Accordingly, such isolated networks, like the LAN, cannot be accessed from the public Internet, but rather only through those computers which are physically connected to the isolated network.

iii. The CIA Group's LAN, and each of its component parts, was maintained in heavily secured governmental facilities, which include multiple access controls and various other electronic and physical security measures.

d. Based on a preliminary analysis of the timestamps associated with the latest (or most recent) creation or modification date associated with the Classified Information, it appears that the Classified Information was copied from the LAN in or about March 2016.

e. The duplication and removal from the LAN of the Classified Information and its subsequent public dissemination via WikiLeaks was not authorized by the United States government.

f. The unauthorized disclosure of the Classified Information could—at a minimum—reasonably be expected to cause serious damage to the national security of the United States. *See* Executive Order 13526; 18 C.F.R. § 3a.11(a)(2).

g. The Classified Information is national defense information and its disclosure could reasonably be expected to be used to the injury of the United States and to the advantage of a foreign nation. *See* 18 U.S.C. § 793(d) & (e).

11. I know, based on my conversations with other law enforcement agents and others, that TARGET SUBJECT JOSHUA ADAM SCHULTE was employed as a computer engineer by the CIA—specifically in the CIA Group—from in or about May 2010 through on or about November 10, 2016, when he resigned from the CIA. Based on those conversations, I understand

the following about the nature of SCHULTE's employment with the CIA, in substance and in part:

a. During SCHULTE's more than six years working in the CIA Group, his responsibilities included, among other things, developing computer code for specific projects, including projects explicitly described in the Classified Information. SCHULTE had a skill set that enabled him to write computer code designed to clandestinely copy data from computers.

b. As part of his responsibilities with the CIA Group, in or about March and early April 2016, SCHULTE was one of three system administrators for the LAN. Among other things, that meant that he was one of three employees responsible for maintaining the LAN, and for controlling the access of other CIA Group employees.

c. These three systems administrators also had "super-user" access to the LAN, which allowed them broader access to programs, files and servers.

12. Based on my conversations with law enforcement officers and others, including individuals with an expertise in computer systems, and knowledge of the LAN, and my conversations with individuals who have conducted preliminary forensic analyses of the LAN and its related computer systems, I understand the following, in substance and in part:

a. Preliminary analysis suggests that the wholesale access to, and subsequent copying of, the Classified Information would likely have required systems administrator access of the type described above.⁵

⁵ I describe this as a "preliminary analysis" because analysis of the precise origin of the Classified Information is ongoing, and therefore the conclusions drawn from the preliminary analyses to date may be subject to modification once the analysis has been concluded. For example, among the facts that the FBI and CIA continue to analyze and verify is the precise number of individuals with "super-user" access who would have had access to the Classified Information during the relevant time period, which in and of itself is in part dependent upon the mechanism or route by which the Classified Information was obtained. Information the FBI received on April 5, 2017 revealed that there is a possibility that this number could have been slightly lower or slightly higher than the initial estimates set forth in prior search warrant affidavits submitted in the course of this

b. The publicly released Classified Information originally published by WikiLeaks, based on a preliminary review, appears to contain the names and/or pseudonyms of, *inter alia*, multiple CIA employees—including two of the three aforementioned LAN systems administrators. SCHULTE's name, on the other hand, apparently was not published in the Classified Information. Thus, SCHULTE was the only one of the three systems administrators who was not publicly identified via WikiLeaks's first publication of the Classified Information.

c. The other two individuals who served in March 2016 as systems administrators for the CIA Group's LAN remain employed by the CIA. SCHULTE resigned from the CIA in November 2016, as described in detail below.

13. Based on my conversations with other law enforcement agents and others, my review of documents prepared by such law enforcement agents or obtained from the CIA, I know that SCHULTE has alleged that, on or about March 1, 2016, another CIA Group co-worker had made a threat against him. Based on those conversations and that review of documents regarding SCHULTE's threat allegations against his former co-worker, I understand the following, in substance and in part:

a. The CIA conducted an investigation into the incident, at the conclusion of which SCHULTE expressed deep unhappiness about the way that CIA responded to the alleged threat.

investigation, and that such variation depends on the route through which the Classified Information was accessed. While there may have been multiple mechanisms to gain access to the Classified Information, the preliminary assessment is that the most likely routes to acquiring that information would have required systems administrator access. Notwithstanding that fact, it is, of course, also possible that an employee who was not a designated systems administrator could find a way to gain access to the Classified Information (*e.g.*, an employee could steal and use—without legitimate authorization—the username and password of a designated systems administrator, or an employee lacking systems administrator access could, at least theoretically, gain access to the Classified Information by finding a “back-door” to it).

b. SCHULTE threatened legal action against the CIA for its handling of the situation, and repeatedly stated that he felt that he was being punished by CIA management for reporting the alleged threat incident.

c. SCHULTE informed CIA security that, if “forced into a corner” he would proceed with a lawsuit against the CIA. He also repeatedly threatened that he or his lawyer would go to the media.

d. In addition, CIA security learned that SCHULTE had removed an internal CIA document from CIA facilities that related to his complaints to the CIA concerning its handling of the alleged threat, despite being told multiple times by CIA security officials not to do so. On or about April 4, 2016, SCHULTE and the other CIA employee were reassigned to different offices within the CIA Group in response to SCHULTE’s allegations.

e. Around the time of his reassignment to another branch within the CIA Group, and at least in part because of his new responsibilities, many of SCHULTE’s administrator privileges on the LAN were revoked, and he was no longer permitted to serve as a systems administrator in the CIA Group’s LAN.

f. At approximately the same time, *i.e.*, on or about April 4, 2016, SCHULTE’s computer access to a specific developmental project (“Project-1”) was also revoked. Until his reassignment, SCHULTE had been the CIA Group employee with principal responsibility for Project-1. Upon SCHULTE’s transfer, principal responsibility for Project-1 was transferred to another CIA Group employee, who received computer access to Project-1.⁶

14. I know from my review of publicly available material on the Internet, including

⁶ SCHULTE retained read-only access to Project-1 (but not the ability to alter the code) and the ability to copy the computer code associated with it in order to support another project for which he had responsibility.

WikiLeaks.org, that Project-1 was one of a small group of CIA projects and capabilities that WikiLeaks highlighted explicitly by name in its March 7, 2017 press release that accompanied the online publication of the Classified Information.

15. Based on my involvement in this investigation and my conversations with other FBI agents involved in this investigation, I know that on or about March 14, 2017, pursuant to a search warrant authorized by the Honorable Barbara Moses, United States Magistrate Judge for the Southern District of New York, Google, Inc. (“Google”) produced information, including a history of TARGET SUBJECT JOSHUA ADAM SCHULTE’s Google searches (the “Google Search(es)” or “Search(es)”).

16. Based on my review of those Google Searches, and conversations with law enforcement agents and others, as well as my own training and experience, I know that on or about April 4, 2016, SCHULTE conducted a Google Search that led him to visit a webpage entitled in part “Detecting USB insertion/Removal in C++ non-GUI application.”⁷ I understand, based on my training, experience, and conversations with others, that “Detecting USB insertion/[r]emoval” likely relates to the function by which a computer recognizes—or does not recognize—that an external device has been connected to it via its USB port. (A USB port is a standard connection interface used to connect devices to a computer, including—among numerous other peripheral items—a portable computer storage device.)

17. Based on my conversations with other law enforcement agents and others, and my review of documents, I understand the following, in substance and in part:

a. On or about April 11, 2016, approximately one week later, SCHULTE

⁷ Both C++ and non-GUI (which stands for graphical user interface) are references to standard types of computer programming language or code, used, inter alia, by aspects of the LAN.

unilaterally, and without authorization, logged onto the CIA Group's LAN and reinstated his own administrator privileges.

b. CIA Group management did not discover that SCHULTE had personally re-instituted his administrator privileges to the LAN without permission until on or about April 14, 2016.

18. Based on my review of the Google Searches, I know that on April 12 and 13, 2016 (*i.e.*, the time period between when SCHULTE reinstated his access to the LAN and FBI's discovery of that unauthorized reinstatement), SCHULTE conducted a series of searches apparently designed to gather information about copying a large quantity of data from one computer storage device to another, including but not limited to the following:

c. On or about April 12 and 13, 2016, in the evening⁸ SCHULTE conducted the following Google Searches, among others:

- i. "windows command line copy all files subdirectories";
- ii. "windows copy all files and subdirectories"; and
- iii. "windows back files xcopy or robocopy"

I understand, based on my training, experience, and conversations with others, that "robocopy" and "xcopy" each refer to computer commands that allow a user to copy multiple computer files—or entire computer directories (and all their contents)—from one computer storage location to another. For example, this command would be used to copy files and folders, *en masse*, from one network to another, from one computer to another, or from a computer network onto a portable

⁸ The Google search warrant returns list the times of the searches in "UTC" or coordinated universal time, which is the same as Greenwich Mean Time. Accordingly, the dates and times of the Google Searches described herein have been adjusted to Eastern Standard Time (*i.e.*, the time zone where SCHULTE conducted the Google Searches).

data blocks or chunks can be of varying sizes. Accordingly, the speed and efficiency of copying data can be affected by the size of each block or chunk of data.

ii. After conducting the above-mentioned Google Search (“optimal reading chunk size c++”), SCHULTE visited websites relating to issues such as “what is the ideal memory block size to use when copying.”

19. Based on my review of the Google Searches, I understand that on or about April 15, 2016, SCHULTE conducted the following Google Search relating specifically to software running on the CIA Group’s LAN: “[] admin view restricted pages.”⁹ After conducting the search, SCHULTE visited websites that related to ways to restrict the ability of even other Systems Administrators to view aspects of the LAN. (SCHULTE conducted the same search again thirteen days later, on or about April 28, 2016.)

20. Based on my conversations with law enforcement officers and others with knowledge of SCHULTE’s personnel file, I understand the following, in substance and in part:

f. On or about April 18, 2016, approximately four days after the CIA had learned of SCHULTE’s unauthorized reinstatement of his systems administrator privileges, SCHULTE received notice regarding CIA policies against personnel restoring their own access to privileges or computer networks after those accesses have been revoked.

g. SCHULTE signed an acknowledgment that he understood that “individuals are not permitted to personally attempt and/or renew their previous authorizations [including administrator privileges] to any particular [computer] system.” That notice further instructed SCHULTE: “do not attempt to restore or provide yourself administrative rights to any project

⁹ The brackets redact out the proprietary name of the specific commercially available software program that was running on the CIA Group’s LAN.

and/or system for which they have been removed.”

21. Based on my review of the Google Searches, and my conversations with other law enforcement officers who have reviewed the Searches, I understand the following, in substance and in part:

a. Also on or about April 18, 2016 (*i.e.*, the same day he was required to sign the acknowledgement of CIA policies), SCHULTE conducted various Google Searches regarding copying files on a computer network, including “copying multiple [] large files.” After conducting this search, SCHULTE visited a website titled, in part, “how to copy a large number of files quickly between two servers.”

b. Less than a week later, on or about April 24, 2016, SCHULTE conducted a Google Search for a “SATA adapter.” Based on my training, experience and conversations with others, I understand that such an adapter is used to connect a computer hard drive to a computer externally, via USB connection. In other words, by connecting an internal drive to another computer via that computer’s external USB port, a SATA adapter allows an internal computer hard drive to be used instead as a portable, external memory drive.

c. On or about April 24, 2016, SCHULTE conducted multiple Google Searches for how to “partition” or divide a computer hard drive up, in order to move files from one storage location on the computer to a separate drive or portioned location.

d. On or about April 28, 2016, SCHULTE again conducted a Google Search relating specifically to software running on the CIA Group’s LAN: “[] admin view restricted pages,” which was identical to the Search, described above, he conducted on April 15, 2016—four days after restoring his own administrator access to that very software program without authorization.

e. On the evening of Saturday, April 30, 2016, SCHULTE conducted numerous Google Searches apparently relating to the deletion of computer data, including possibly his own Google Searches, which searches included the following:

- i. “google history”;
- ii. “google view browsing history”;
- iii. “western digital disk wipe utility”; and
- iv. “Samsung ssd wipe utility”

I know, based on my training, experience and conversations with others, that “[W]estern [D]igital” is the name of one of the largest providers of computer storage hardware (such as portable hard drives), and that “wipe utility,” or wipe drive utilities are, based on the description on Western Digital’s website, designed to “erase all the data on a hard drive.” I further know, based on my training, experience and conversations with others, that Samsung SSD is a reference to a brand (Samsung) of solid-state drives, which is a type of portable computer hard drive.

22. Based on my involvement in this investigation, and my conversations with other law enforcement officers involved in this investigation, I know the following, in substance and in part:

a. On March 15, 2017, the Honorable Barbara C. Moses issued a search warrant (the “March 15 Search Warrant”) for a Manhattan apartment located at 200 East 39th Street, Apartment 8C, New York, New York 10016, in which SCHULTE has resided since shortly after his resignation from the CIA in November 2016 (the “Residence”).¹⁰

¹⁰ Previously, on March 13, 2017, Judge Moses had issued a search warrant for the same premises. The Government sought a second search warrant for an overt search of the premises because the March 13 search warrant had been executed covertly on or about March 14, 2017 and agents were not able to complete the search.

b. Pursuant to the search conducted on that same day, law enforcement officers recovered, among other things, numerous computer storage devices with the capacity to store at least more than ten terabytes of data, including multiple Western Digital hard disk drives (themselves totaling multiple terabytes¹¹ of storage space) and at least one Samsung SSD solid state external hard drive.¹² As noted immediately above, these are the two brands of hard drive which SCHULTE specifically searched for “wipe utilities”—programs designed to completely erase data from the drives—on the evening of April 30, 2016.¹³

23. Based on my review of the Google Searches, and my conversations with other law enforcement officers who have reviewed the Searches, I understand the following, in substance and in part:

c. At approximately 3:20 a.m. in the early morning hours of May 1, 2016 (*i.e.*, approximately five hours after conducting the Google Searches regarding the wiping of hard drives described in Paragraph 21(e) above), SCHULTE visited a website entitled in part “how can I verify that a 1tb file transferred correctly.” I know, based on my training, experience and conversations with others, that “1tb” likely refers to 1 terabyte of data.

d. Three days later, on or about May 4, 2016, SCHULTE again conducted

¹¹ I know, based on my training, experience and conversations with others, that one terabyte of data is roughly equivalent to one-thousand gigabytes of data or one-million megabytes of data. Put differently, one terabyte of data is roughly equivalent to more than 85 million word processing pages.

¹² Those computer devices are in the process of being analyzed.

¹³ In addition, pursuant to the search, agents recovered from SCHULTE’s apartment, internal correspondence from the CIA that appears, based on a preliminary analysis, to contain classified information (though *not* the Classified Information), including, *inter alia*, the names of CIA employees, and code names of specific CIA Group programs. I know, based on my training, experience and conversations with others, that removing and storing classified information in one’s own home is generally prohibited.

multiple Google Searches apparently related to the permanent deletion of data from a computer storage device, including “western digital disk wipe utility” and “can you use dban on ssd.” Based on my training, experience and conversations with others, I understand that:

i. “SSD” is an acronym for “solid-state drive” a kind of computer memory storage device.

ii. “dban” is an acronym that stands for “Darik’s Boot and Nuke,” a computer software program that is designed, according to various websites selling the software, to “securely wipe[] the hard disks of most computers. DBAN is appropriate for bulk or emergency data destruction.” According to one popular technology website, CNET.com: “use DBAN only if you want to completely eradicate any trace of data on a hard drive. This is the ultimate in data shredding—there’s no recovery once you’ve used it.”

e. Starting two days later, May 6, 2016, and again on May 8, 2016, SCHULTE conducted multiple Google Searches apparently designed to research the anonymous transmission of data on the Internet, through the use of so-called “private trackers,” which are non-public Internet sites set up to privately transfer large quantities of data from one computer to another, as well as through “The Onion Router” or “TOR,” which allows for anonymous communications on the Internet via a worldwide network of linked computer servers, and multiple layers of data encryption.

f. On May 6, 2016, SCHULTE conducted multiple Google Searches apparently relating to ways to transfer data between computers anonymously, including searches for “trackers,” “trackers torrent,” and “private trackers.” Based on my training, experience and conversations with others, I understand that trackers or torrent trackers are computer code (or a “protocol”) that connects computers on the Internet to each other in order to facilitate the transfer

of large files over the Internet. I further understand that “private trackers” are trackers that are not publicly accessible, but rather that require authorization by an administrator to use the tracker to share files. After conducting the Google Search for “private trackers,” SCHULTE visited a website entitled “opentrackers.org,” which claims that its private tracker can be used “to avoid detection & bypass anti-piracy/site blocking.”¹⁴

g. On May 8, 2016, SCHULTE conducted multiple Google Searches apparently related to the use of The Onion Router (or TOR) to anonymously transfer encrypted data on the Internet. For example, SCHULTE searched for “setup for relay,” “test bridge relay,” and “tor relay vs bridge.” Each of these searches returned information regarding the use of interconnected computers (or relays) on TOR to convey information, or the use of a computer to serve as the gateway (or bridge) into the TOR network of relays.

24. Based on my conversations with law enforcement officers and others with knowledge of SCHULTE’s personnel file and computer access, I understand the following, in substance and in part:

a. On May 26, 2016 (*i.e.*, less than three weeks after he conducted Google Searches related to the use of TOR as described in Paragraph 23 above), and notwithstanding the warnings described above, SCHULTE made an official request that he again be given full access to Project-1.

b. Before receiving an official response to that request, SCHULTE requested access from another employee who, apparently without proper vetting, granted SCHULTE the

¹⁴ Trackers and torrent trackers are often used in the transfer of large media files, including video and audio. The investigation to date has indicated that, in addition to the activity set forth in this section, SCHULTE also appears to have been engaged in the sharing of large media files, including, among other things, movies and music. Accordingly, it is at least possible that certain of these searches, as well as others described herein, could relate to those activities.

requested full access to Project-1.

c. On the same day, SCHULTE used that newly obtained access to, unilaterally and without authorization, revoke the computer access permissions of all other CIA Group employees to work on Project-1.

d. Once this conduct was discovered, SCHULTE was issued a letter of warning that stated, "You were aware of the policy for access and your management's lack of support for you to retain administrative privileges, but nonetheless you took steps to deliberately violate that policy and gain those privileges." It continued by warning SCHULTE that any future violations would result in "further administrative action of a more severe nature." After receiving the letter of warning, SCHULTE disagreed with some of its conclusions and consequently refused to sign the form.

25. Based on my review of the Google Searches, and my conversations with other law enforcement officers who have reviewed the Searches, I understand the following with respect to TARGET SUBJECT JOSHUA SCHULTE's searches related to Wikileaks, in substance and in part:

a. For the approximately six years between at least August 2010 and August 3, 2016, he conducted no searches for WikiLeaks.

b. But, beginning on August 4, 2016, SCHULTE initiated numerous Google Searches for WikiLeaks and related terms, and visited more than 200 pages that he apparently found as a result of those searches.

c. Between August 4 and August 22, 2016, SCHULTE conducted Searches for "wikileaks" at least eleven times. Pursuant to those Google Searches, he read dozens of articles regarding WikiLeaks, though he appears never to have actually visited the WikiLeaks.org Internet

website.¹⁵

d. Between August 2016 and March 14, 2017, he searched “wikileaks” at least a dozen additional times, and read hundreds of online articles and publications regarding WikiLeaks. He apparently first visited the WikiLeaks.org website on March 7, 2017—the date of the release of the Classified Information.

e. In addition to the numerous searches for “wikileaks” which commenced on August 4, 2016, SCHULTE also conducted multiple related Searches, including: prior to the March 7, 2017 release of the Classified Information, “assange” (Julian Assange is the founder and “editor-in-chief” of WikiLeaks.org), “snowden its time,” “wikileaks code,” and “wikileaks 2017”—and after the March 7, 2017 release of the Classified Information, “wikileaks public opinion,” and “officials were aware before the WikiLeaks release of a loss of sensitive information.”

26. Based on my review of the Google Searches, and my conversations with other law enforcement officers who have reviewed the Searches, I further understand the following, in substance and in part:

a. On August 1, 2016, SCHULTE conducted a Google Search for “create temporary email,” and, three seconds later, visited the website www.throwawaymail.com. Based on my training, experience, conversations with others, and review of documents, I know that “throwawaymail.com” is an Internet website that randomly generates an anonymous email address for a user without any registration; that random and anonymous email address can immediately

¹⁵ I know, based on my training, experience, and conversations with others, that, among many other reasons, one reason a person might search for “wikileaks” but never visit the website is because the act of visiting a website can leave a trail that a particular IP address visited the website. Accordingly, one reason (perhaps among many) for repeatedly searching “wikileaks” but not visiting the WikiLeaks.org website, would be to avoid leaving behind a footprint of one’s visit.

receive and send emails, but automatically expires within a very short period of time (approximately 48 hours).

b. On August 10, 2016, SCHULTE conducted a Search for “tails,” and then, two seconds later, visited the website “<https://tails.boum.org>.” I know, based on my training, experience, conversations with others, and review of that website, that “tails” is an acronym for “the Amnesic Incognito Live System,” that works in conjunction with TOR (described above) to ensure anonymous connections on the Internet and therefore will leave no digital footprint of the internet websites visited by someone using the system.¹⁶ The WikiLeaks.org website also lists “tails” as one of its “partner organizations.”

c. On August 14, 2016, SCHULTE searched various topics regarding employment litigation and disputes, including filing a lawsuit against one’s boss (*e.g.* “can you sue your boss”), one’s employer (*e.g.* can i sue my employer for unfair treatment”), and the “EEOC.” (Less than an hour after conducting those Searches, SCHULTE searched “tor.”)

d. On September 1 and 5, 2016, SCHULTE repeatedly searched, “what is a mole.” I know, based on my training and experience that, among other meanings, a “mole” generally refers to a spy working inside a country’s security, military or intelligence services.

27. Based on my conversations with law enforcement officers and others familiar with TARGET SUBJECT JOSHUA SCHULTE’s employment history with the CIA, including his

¹⁶ News reporting indicates that Edward Snowden used the tails system in connection with his transfer of allegedly classified documents to various news outlets. *See* Out in the Open: Inside the Operating System Edward Snowden Used to Evade the NSA, Wired, April 14, 2014, *available at* <https://www.wired.com/2014/04/tails/> (last accessed Mar. 31, 2017); The ultra-secure Tails OS beloved by Edward Snowden gets a major upgrade, PC World, Jan. 27, 2016, *available at* <http://www.pcworld.com/article/3026721/linux/the-ultra-secure-os-beloved-by-edward-snowden-gets-a-major-upgrade.html> (last accessed Mar. 31, 2017).

security clearances and related investigations, I understand the following, in substance and in part:

a. In approximately August 2016, as part of a standard background reinvestigation of SCHULTE for the purpose of renewing his security clearances, the CIA conducted interviews of multiple CIA Group colleagues. Among other things:

b. Some (but not all) colleagues independently reported that SCHULTE's demeanor with his management and colleagues, and his commitment to his work, changed markedly for the worse in or around February 2016.

c. Multiple colleagues stated that SCHULTE had indicated that he felt aggrieved by the CIA in a number of respects. Some also reported that they believed SCHULTE to be untrustworthy and potentially subject to outside coercion. (Other colleagues made no such report and, indeed affirmatively reported that they believed that SCHULTE was, in fact, trustworthy.)

d. Some (but not all) colleagues also reported that SCHULTE's security practices were lax, and that SCHULTE tended not to abide by security guidelines he deemed inconvenient—particularly guidelines concerning when and what kinds of media or data (such as external drives) could be connected or uploaded to CIA computer systems.¹⁷

28. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know in substance and in part that, in connection with and preceding SCHULTE's November 2016 resignation from the CIA:

a. Approximately one month prior to his resignation, on October 12, 2016, SCHULTE, using his CIA email account, sent an email to another CIA Group employee at that

¹⁷ As described herein, external drives can be connected to computers and files in order to allow users to move files from the computers onto the portable external drives.

employee's official email account. The subject line of the email stated, "ROUGH DRAFT of Resignation Letter *EYES ONLY*." The email contained a letter entitled "Letter of Resignation 10/12/16" and addressed to "To whomever it may concern" ("Draft Resignation Letter"). I know from reviewing the Draft Resignation Letter, which spanned approximately three single-spaced pages, the following:

i. SCHULTE began the letter by stating, in substance and in part, that he had "always been a patriot" and would "obviously continue to support and defend this country until the day that I die," but that "from this day forward" he would "no longer do so as a public servant."

ii. SCHULTE claimed that he believed that the CIA Group management had unfairly "veiled" CIA leadership from various of SCHULTE's previously expressed concerns, including concerns about the network security of the CIA Group's LAN. SCHULTE continued: "That ends now. From this moment forward you can no longer claim ignorance; you can no longer pretend that you were not involved."

iii. SCHULTE explained that he was resigning from the CIA because CIA Group management had, among other things, "ignored" issues he had raised about "security concerns" and had attempted to "conceal these practices from senior leadership," including that the CIA Group's LAN was "incredibly vulnerable" to the theft of sensitive data. He claimed that one named CIA Group manager had ignored his security concerns and "later attempt[ed] to evade responsibility and blame the decentralized and insecure [CIA Group computing] environment entirely on me."¹⁸

¹⁸ SCHULTE went on to describe other complaints he had about managers at the CIA. Among other things, SCHULTE described his complaints about the way in which CIA Group management had handled various personnel and disciplinary issues.

iv. Specifically, SCHULTE wrote that inadequate CIA security measures had “left [the CIA Group’s LAN] open and easy for anyone to gain access and easily download [from the LAN] and upload [sensitive CIA Group computer code] in its entirety to the [public] internet.”

b. It appears that SCHULTE did not, in fact, submit the Draft Resignation Letter to the CIA.

c. On his last day with the CIA (November 10, 2016), SCHULTE did, however, send an internal email to the CIA Office of the Inspector General (OIG) advising that he had been in contact with the United States House of Representatives’ Permanent Select Committee on Intelligence regarding his complaints about the CIA (the “OIG Email”).

i. In the OIG Email, which SCHULTE labeled “Unclassified,” SCHULTE raised many of the same complaints included in the draft “Letter of Resignation 10/12/16,” described above, including the CIA’s treatment of him and its failure to address the “security concerns” he had repeatedly raised in the past.

ii. Shortly thereafter, CIA security learned that one of SCHULTE’s colleagues had witnessed SCHULTE printing the OIG Email, placing it in a folder, and exiting the CIA Component facility where SCHULTE worked. Notwithstanding SCHULTE’s labeling of the email as “Unclassified,” the CIA subsequently determined that the OIG Email, which SCHULTE removed from the CIA without authorization, did in fact contain classified information.

29. Based on my involvement in this investigation, and my conversations with other law enforcement officers involved in this investigation and/or my review of reports prepared in the course of this investigation, I understand that the FBI recovered a copy of the November 10, 2016 OIG Email, which contained classified information and which SCHULTE labeled

“Unclassified” and removed from a CIA facility, from his residence during the March 15, 2017 search.

B. Probable Cause Relating to CP Offenses

30. As described above, On March 15, 2017, the Honorable Barbara C. Moses issued a search warrant to search SCHULTE’s residence in Manhattan—the March 15 Search Warrant. Based on my involvement in this investigation, and my conversations with other law enforcement officers involved in this investigation as well as my review of documents prepared in the course of this investigation, I understand the following, in substance and in part:

a. During the execution of the March 15 Search Warrant, law enforcement officers recovered, among other things, multiple computers, servers, and other portable electronic storage devices (the “Schulte Devices”). Following the seizure of the Schulte Devices, the devices were transported by the FBI for analysis and examination to a U.S. Government facility in Herndon, Virginia, within the Eastern District of Virginia.

b. In the course of searching the Schulte Devices for evidence, fruits, and instrumentalities of the National Security and Computer Crime Offenses, agents discovered a photograph on SCHULTE’s desktop computer that appeared to depict child pornography (the “CP Picture”). An agent who is assigned to the Crimes Against Children Squad (the “CACS Agent”) reviewed the CP Picture and believed that the CP Picture depicted a naked young child on all fours and what appear to be two adults around her, one of whom appears to be performing a sexual act on the child—oral sex around the child’s buttocks. The CACS Agent also believed that the child was a minor based on, among other things, body structure, lack of breast development, and lack of pubic hair.¹⁹

¹⁹ Although the CACS Agent believed the CP Picture was an actual photograph, he stated that it is possible that the CP Picture may have been altered. However, I understand that the CACS Agent

C. Probable Cause for Evidence of Copyright Offenses

31. Based on my conversations with members of the FBI who were involved in searching the Schulte Devices for evidence, fruits, and instrumentalities of the National Security and Computer Crime Offenses pursuant to prior search warrants, I have learned, among other things, that at least one of the servers recovered from SCHULTE's Manhattan residence ("Server-1") has indications that SCHULTE was involved in illegally sharing copyrighted movies over the Internet. Specifically, Server-1's command log (which shows the history of commands sent to Server-1 by the user, likely via a computer connected to Server-1), indicates that SCHULTE participated in the sharing of dozens of movies using torrent trackers.²⁰ As described above, based on my training, experience and conversations with others, I understand that torrent trackers are computer protocol which connect computers on the Internet to each other in order to facilitate the transfer of large files over the Internet.

32. Based on my training, experience, and my conversations with another FBI agent who has reviewed the public catalog of copyrighted works available through the United States Copyright Office, I know that most, if not all, of the movies that SCHULTE appears to have participated in sharing are copyrighted works registered with the United States Copyright Office. For example, among the many movies that were apparently shared include *Hacksaw Ridge*; *The*

reviewed a printout of the CP Picture. The printout of the CACS Picture had the effect of magnifying the photograph, which makes it look slightly different than what is on the Desktop Computer. An agent involved in this investigation has reviewed the CP Picture on the Desktop Computer and believes that it is an actual photo.

²⁰ Upon viewing the command log, which was searched pursuant to a prior search warrant for evidence regarding the National Security and Computer Crime Offenses, and upon seeing indications of illegal movie sharing, members of the FBI stopped viewing the command log and contacted the U.S. Attorney's Office.

Revenant; *Captain America: Civil War*; and *The Hateful Eight*, all of which are copyrighted works currently registered with the United States Copyright Office.

33. Based on my involvement in this investigation as well as my review of reports prepared in the course of this investigation, I understand that in or about March 2017, FBI agents conducted interviews of multiple CIA employees who know SCHULTE, and that, among other things, one of those employees stated that SCHULTE operates a service allowing users to stream movies over the Internet (the “Streaming Service”) and that SCHULTE manages the accounts of users of the Streaming Service.

34. Based on my review of a telephone that was among the Schulte Devices for evidence, fruits, and instrumentalities of the National Security and Computer Crimes Offenses pursuant to the terms of the March 15 Search Warrant, I have learned, among other things, that on or about October 31, 2016, SCHULTE sent an email to approximately 20 other individuals with the subject line “Pedbsktbll Plex Server Downtime 11/9/2016-1/2017” (the “Email”). In the Email, SCHULTE notifies the recipients that the “server will be down as it relocates to NYC starting 11/9. Thus, you will have the next 9 days to select and download material you may wish to watch during that downtime. Hopefully, the server will be back and running mid to late December – January at the latest.” Based on my training, experience, and participation in this investigation, I believe that SCHULTE was referring to the Streaming Service and was alerting users that the service would be unavailable while he moved to New York in late 2016, at which point (as explained below) he started his employment at the Subject Premises.

D. Probable Cause Justifying Search of the Subject Premises

35. I know from speaking to a representative of Bloomberg LP (the “Company”) that SCHULTE has been employed with the Company since November 14, 2016 and that since that time he has worked at the Company’s office located at the Building described above in paragraph

3. I also know that SCHULTE has a designated workspace located at Workstation 173 on the 16th floor of the Building, *i.e.*, Subject Premises-1, and that Subject Premises-1 contains a desktop computer that was used by SCHULTE (the “Desktop Computer”).

36. On or about March 15, 2017, approximately one week after the March 7 publication of the Classified Information described above, I and another FBI agent approached SCHULTE in the lobby of the Building. We identified ourselves as law enforcement, and asked SCHULTE whether he would be willing to speak with us concerning the March 7, 2017 publication by Wikileaks. Based on my participation in that interview, I understand the following, in substance and in part:

a. SCHULTE agreed to be interviewed, and acknowledged that he left the CIA in November 2016 out of frustration with way things were run there, and began working for the Company.

b. SCHULTE denied any involvement in the transmission of the Classified Information to WikiLeaks.

c. During the interview, SCHULTE had a backpack in his possession, and he informed agents that his passport was inside the backpack. SCHULTE declined at that time to consent to a search of his backpack (the “Backpack”), although he showed agents a set of documents retrieved from his backpack that confirmed SCHULTE was traveling overseas the following day (March 16, 2017).

d. Another FBI agent informed SCHULTE that the FBI would soon be executing a search of SCHULTE’s residence (*i.e.*, the March 15 Search Warrant). SCHULTE subsequently provided the FBI access to his residence and remained near his residence while the search was being conducted.

e. SCHULTE informed agents that he had inside his apartment a diplomatic passport (in addition to the personal passport inside his backpack) that he had not returned to the CIA upon his resignation. Between approximately 10 p.m. and 11 p.m. on March 15, 2017, while the March 15 Search Warrant was being executed, SCHULTE left the vicinity of his residence and informed agents that he would return at 11:30 p.m. to get an update on the progress of the search.

37. Based on my participation in this investigation, and my conversations with other law enforcement officers who conducted surveillance of TARGET SUBJECT JOSHUA ADAM SCHULTE on the night of March 15, 2017, I understand the following, in substance and in part:

a. After SCHULTE departed the vicinity of the Schulte Residence, law enforcement learned that SCHULTE had entered the Building where Subject Premises-1 is located (*i.e.*, 120 Park Avenue, New York, New York).

b. I know from my conversations with other FBI agents involved in this investigation that the Company's corporate security department confirmed that SCHULTE, in fact, had proceeded to use his desktop computer located at Subject Premises-1.

38. As of approximately 12:15 a.m., SCHULTE had not returned to the residence where the March 15 Search Warrant was still being executed. I and another FBI agent proceeded to the Building, and witnessed SCHULTE proceeding down an escalator to the lobby of the Building. SCHULTE was carrying the Backpack. After I and another FBI agent witnessed SCHULTE proceed to the lobby of the Building, we approached SCHULTE and asked him if he would be willing to speak with us. Based on my participation in that conversation, I understand the following, in substance and in part:

a. Schulte agreed to speak with us.

b. We informed SCHULTE that a copy of the November 10, 2016 OIG Email,

which contained classified information, had been found inside his residence, and that he was being investigated for, among other things, the unlawful retention of classified information.

c. We also informed SCHULTE (whom the FBI knew had scheduled overseas travel for March 16, 2017) that we were requesting his passports, including SCHULTE's diplomatic passport, which had not been found in the search of SCHULTE's residence.

d. SCHULTE, who was not placed under arrest but was told he had a right to seek advice from an attorney, was told that he could face arrest if he did not agree to surrender his passports. SCHULTE agreed to provide his passports to the FBI and stated that both his personal passport (which SCHULTE previously informed us had been in the Backpack earlier that night) and his diplomatic passport were upstairs at his Company workstation. SCHULTE was accompanied by FBI agents and Company security to his workstation (*i.e.*, Subject Premises-1), where he retrieved his passports.²¹

e. SCHULTE also consented to a search of his Backpack at that time.

39. I believe, based on the foregoing, that when SCHULTE proceeded from his residence to his workstation at the Company, *i.e.*, Subject Premises-1, he placed at least one of his passports in Subject Premises-1. Because SCHULTE did not consent to a search of the Backpack until after he had already visited Subject Premises-1, I believe that SCHULTE also may have placed other items from his Backpack in Subject Premises-1 and/or stored other personal items in Subject Premises-1.

40. I know from information provided by the Company that, following the above events, SCHULTE, who remains employed with the Company, was placed on temporary paid

²¹ SCHULTE ultimately retained counsel, who also agreed on SCHULTE's behalf to allow the FBI to temporarily retain SCHULTE's passports.

leave beginning on March 16, 2017. I also know that, since March 16, 2017, *i.e.*, the date when SCHULTE last reported to Subject Premises-1, that the items within Subject Premises-1 were preserved. In other words, the Company did not take steps to clear out or alter the materials located at Subject Premises-1, and the workspace was not reassigned to any other employee or designated for any other purpose.

41. To the knowledge of a senior Company representative who is aware of the existence of this investigation, Subject Premises-1 has not been altered since March 16, 2017. However, Company officials removed the hard drive of SCHULTE's desktop computer—Subject Premises-2—and stored that hard drive in a secure location at the Company. On May 5, 2017, pursuant to a subpoena issued by a grand jury sitting in this District, the Company transferred Subject Premises-2 to the custody of the FBI. Subject Premises-2 remains in the FBI's custody in the Southern District of New York.

42. I also understand from information obtained provided by the Company that, following the above events, the Company, among other things, analyzed SCHULTE's electronic and telephonic communications while at the Subject Premises in the days leading up to March 16, 2017, when SCHULTE was last seen at the Subject Premises.

43. Based on my training and experience, I know that individuals who are involved in the Subject Offenses often use computers and other electronic devices in furtherance of their criminal activities. Based on my training and experience, I also know that individuals typically keep their computers and other electronic devices in their homes, their persons, or other areas where the devices can be stored or used. Oftentimes materials relating to the Subject Offenses may be kept on electronic storage media, such as thumb drives, external hard drives, mp3 players, SD cards, or other forms of easily concealed electronic storage devices.

44. Based on my training and experience, I also know that individuals who engage or otherwise are involved in the Subject Offenses often take steps to ensure that information they may have obtained unlawfully is not obtained by law enforcement. Among other things, I know that such individuals oftentimes will maintain some of the more sensitive materials on their person or in another location, such as their private workspace at their place of employment, to ensure that they are not inadvertently discovered or otherwise found by law enforcement or other individuals.

45. As noted above, individuals who engage in Subject Offenses often use computers and other electronic devices to store documents and records relating to their illegal activity. Individuals engaged in these activities use electronic devices to, among other things, store copies of documents or materials relating to the illegal activity (including, among other things, classified documents, child pornography, and evidence of copyrighted works); engage in email correspondence relating to their illegal activity; store contact information of co-conspirators, including telephone numbers, email addresses, and identifiers for instant messaging and social medial accounts; and/or store records of illegal transactions (including, among other things, illegal transactions involving classified documents, child pornography, and copyrighted works).

46. Individuals who engage in the criminal activity described herein, in the event that they change computers, will often back up or transfer files from their old computers' hard drives to that of their new computers, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity. In addition, individuals who engage in such criminal activity will often also store or transfer files on electronic storage media other than computer hard drives, including thumb drives, flash memory cards, CD-ROMs, or portable hard drives to, for example, facilitate the use of the information or to transfer it to co-conspirators in support of the criminal scheme.

47. Individuals who engage in criminal activity involving computers and electronic devices also often maintain physical evidence of their criminal activity, including, among other things, printouts of documents and records that are also stored electronically, as described above, or handwritten notes of the same, for example as a backup in case of a failure of the electronic media on which they were stored or to facilitate use of the data.

48. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files can be stored on a hard drive for years at little or no cost. Even when such files have been deleted, they can often be recovered, depending on how the hard drive has subsequently been used, months or years later with forensics tools. Specifically, when a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Deleted files, or remnants of deleted files, may accordingly reside in “slack space” (space that is not being used for storage of a file) for long periods of time before they are overwritten. In addition, a computer’s operating system may keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are generally automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve from a hard drive or other electronic storage media depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits.

49. Based on my training, experience, and discussions with other FBI agents, I also know that, with respect to the CP Offenses in particular:

a. Persons who collect and distribute child pornography frequently collect and view sexually explicit materials in a variety of media, such as photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media that they use for their own sexual arousal and gratification. These examples of visual media containing sexually explicit materials are often times stored on various devices, including but not limited to, computers, disk drives, servers, modems, thumb drives, personal digital assistants, mobile phones and smart phones, digital cameras, and scanners, and the data within the aforesaid objects relating to said materials.

b. In addition, I know that individuals who collect and distribute child pornography, in the event that they change computers, will often back up or transfer files from their old computers' hard drives to that of their new computers, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity. In addition, individuals who engage in such criminal activity will often also store or transfer files on electronic storage media other than computer hard drives, including thumb drives, flash memory cards, CD-ROMs, or portable hard drives to, for example, facilitate the use of the information or to transfer it to co-conspirators in support of the criminal scheme.

c. I also know that the child pornography detailed above was likely downloaded via the Internet. As a result, electronic devices (including electronic devices within Subject Premises-1) may contain messages, emails, photographs, and/or videos relating to the possession, receipt, or production of child pornography. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files can be stored on a hard drive for years at little or no cost. Even when such files have been deleted, they can often be recovered, depending on how the

hard drive has subsequently been used, months or years later with forensics tools. Specifically, when a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Deleted files, or remnants of deleted files, may accordingly reside in “slack space” (space that is not being used for storage of a file) for long periods of time before they are overwritten. In addition, a computer’s operating system may keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are generally automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve from a hard drive or other electronic storage media depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits.

50. Based on the foregoing, I respectfully submit that there is probable cause to believe that SCHULTE is committing or has committed the Subject Offenses, and that evidence of this criminal activity is likely to be found in Subject Premises-1 (including on electronic devices located therein) and on Subject Premises-2. As a result, I am seeking authorization for a search warrant to search the Subject Premises for evidence of the Subject Offenses, including the items set forth in Attachment A.

III. Items to Be Seized

51. Closed or Locked Containers. Based on my training, experience, participation in this and other investigations, I know that individuals who participate in criminal activities routinely secrete and store books, records, documents, currency and other items of the sort described in Attachment A in secure locations, including locked or closed containers, in an effort to prevent the discovery or theft of said items. The requested warrant and search procedure includes a search of

any closed containers in Subject Premises-1, including cabinets, drawers, and other appurtenances located on or within Subject Premises-1 whether they are locked or unlocked.

52. Electronic Devices. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the requested warrants would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. Based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, thumb drives, magnetic tapes and memory chips. I also know that during the search of Subject Premises-1 in particular, it may not be possible to fully search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process, which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.

b. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of Subject Premises-1. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 160

gigabytes (GB) of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 80 million pages of data, which, if printed out, would result in a stack of paper over four miles high.

c. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

53. In light of these concerns, I hereby request the Court’s permission to copy information stored on computer hardware (and associated peripherals) that may contain some or all of the evidence described in Attachment A hereto, and to conduct an off-site search of such copies for the evidence described, using the general procedures described in Attachment A. With respect to Subject Premises-2 (which has already been provided to the FBI pursuant to a subpoena), and to the extent law enforcement is unable to copy other electronic devices located at Subject Premises-1, I hereby request the Court’s permission to seize those devices and search them off-site.

IV. Procedures for Searching ESI

A. Execution of Warrant for ESI

54. Federal Rule of Criminal Procedure 41(e)(2)(B) provides that a warrant to search for and seize property “may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information . . . for later review.” Consistent with Rule 41, this application requests authorization to search Subject Premises-2, which is in the custody of the FBI, and to search and/or seize any other electronic storage media, including thumb drives, flash memory cards, CD-ROMs, or portable hard drives located in Subject Premises-1, and transport them to an appropriate law enforcement facility for review. This is typically necessary for a number of reasons:

- First, the volume of data on computer devices and storage media is often impractical for law enforcement personnel to review in its entirety at the search location.
- Second, because computer data is particularly vulnerable to inadvertent or intentional modification or destruction, computer devices are ideally examined in a controlled environment, such as a law enforcement laboratory, where trained personnel, using specialized software, can make a forensic copy of the storage media that can be subsequently reviewed in a manner that does not change the underlying data.
- Third, there are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized personnel and equipment potentially required to safely access the underlying computer data.
- Fourth, many factors can complicate and prolong recovery of data from a computer device, including the increasingly common use of passwords, encryption, or other

features or configurations designed to protect or conceal data on the computer, which often take considerable time and resources for forensic personnel to detect and resolve.

55. As discussed herein, the Company is a functioning company that conducts legitimate business. The seizure of the Company's computers or other storage media may limit the Company's ability to conduct its legitimate business. In order to execute the warrant in the most reasonable fashion, law enforcement personnel will attempt to investigate on the scene of what computers or storage media must be seized or copied, and what computers or storage media need not be seized or copied. Law enforcement personnel will speak with Company personnel on the scene as may be appropriate to accomplish this. Where appropriate, law enforcement personnel will copy data, rather than physically seize computers, to reduce the extent of any disruption of the Company's business operations. If employees of the Company so request, the agents will, to the extent practicable, attempt to provide the employees with copies of data that may be necessary or important to the continued functioning of the Company's legitimate business. If, after inspecting the seized computers off-site, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the Government will return it.

B. Review of ESI

56. Following the search of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained therein for information responsive to the warrant.

57. In conducting this review, law enforcement personnel may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- conducting a file-by-file review by “opening” or reading the first few “pages” of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);
- “scanning” storage areas to discover and possibly recover recently deleted data or deliberately hidden files; and
- performing electronic keyword searches through all electronic storage areas to determine the existence and location of search terms related to the subject matter of the investigation. (Keyword searches alone are typically inadequate to detect all information subject to seizure. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.)

58. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement personnel may need to conduct a complete review of all the ESI from searched devices or storage media to evaluate its contents and to locate all data responsive to the warrant.

C. Return of ESI

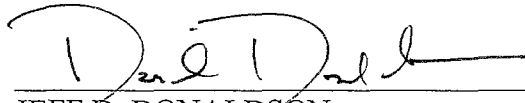
59. If the Government seizes any electronic devices, later determines that the electronic devices are no longer necessary to retrieve and preserve the data, and the items are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return these items, upon request. Computer data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the

offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the Subject Offenses.

V. Conclusion and Ancillary Provisions

60. Based on the foregoing, I respectfully request the court to issue a warrant to search and seize the items and information specified in Attachment A to this Affidavit and to the Search and Seizure Warrant.

61. In light of the confidential nature of the continuing investigation, I respectfully request that this Affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise.


JEFE D. DONALDSON
Special Agent
Federal Bureau of Investigation

Sworn to before me on
this 5th day of May 2017


THE HONORABLE SARAH NETBURN
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK

Attachment A

I. Premises to be Searched—Subject Premises

The premises to be searched (the “Subject Premises”) is described as follows, and includes all locked and closed containers found therein:

- Workstation number 173 (“Workstation 173”) on the 16th floor of the offices of Bloomberg L.P., located at 120 Park Avenue, New York, New York 10017, which is an office space within a tan commercial high-rise office building (the “Building”) located on the Northwest corner of Park Avenue and East 41st Street in Manhattan, as well as any closed containers or items contained therein or related thereto (“Subject Premises-1”), including but not limited to any servers that contain images or back-up copies of any electronic media (as defined herein) contained within or assigned to Workstation 173, or electronically generated logs of activity conducted within Workstation 173, to the extent such servers or electronically generated logs are maintained by Bloomberg L.P. The exterior of the Building has a glass entrance with the number “120” visible from the exterior.
- A computer hard drive, which presently is in the possession, custody, and control of the FBI in the Southern District of New York, known and described as: a Samsung internal solid state drive with model number MZ-HPU512T/0H1 and serial number S1L5NYAG301784 (the “Subject Premises-2”) (collectively, with Subject Premises-1, the “Subject Premises”).

II. Items to Be Searched and Seized

A. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be searched and/or seized from the Subject Premises include the following evidence, fruits, and instrumentalities of: (i) the unauthorized possession and, *inter alia*, the communication of national defense information to someone not entitled to receive it, in violation of Title 18, United States Code, Section 793(d); the unlawful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); exceeding authorized access to a computer in order to obtain national defense information with reason to believe that information could be used to the injury of the United States and the advantage of a foreign nation and willfully transmitting that information to a person not entitled to receive it, in violation of Title 18, United States Code, Section 1030(a)(1); intentionally exceeding authorized access to a

computer and thereby obtaining information from a department or agency of the United States, in violation of Title 18, United States Code, Section 1030(a)(2)(B) (the “National Security and Computer Crime Offenses”); (ii) violations of Title 18, United States Code, Section 2252 (possession, transportation, receipt, distribution, production, and reproduction of sexually explicit material relating to children) and Title 18, United States Code, Section 2252A (activities relating to material constituting or containing child pornography) (the “CP Offenses”); and (iii) violations of Title 17, United States Code, Section 506 and Title 18, United States Code, Section 2319 (criminal infringement of a copyright) (the “Copyright Offenses”) (collectively, with the National Security and Computer Crime Offenses and the CP Offenses, the “Subject Offenses”), described as follows:

1. Evidence, fruits, and instrumentalities of each of the Subject Offenses that is presently, or was on or about March 15 and 16, 2017 and before, located in or around Workstation 173 on the 16th floor of the offices of Bloomberg L.P., located at 120 Park Avenue, New York, New York 10017, including:

- a. Evidence concerning the identity or location of, and communications with, any co-conspirators.
- b. Any and all notes, documents, records, correspondence, or materials, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, and handwritten notes), pertaining to the Subject Offenses.
- c. Electronic devices (including but not limited to computers, tablets, smartphones, and cellular telephones) and storage media used in furtherance of Subject Offenses, containing evidence of the Subject Offenses, or containing evidence authorized for seizure in subparagraphs (a) and (b), above. The term “storage media” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

2. Electronic forensic evidence relating to each of the Subject Offenses, including for any electronic device or storage media whose search and/or seizure is authorized by this warrant as described above in paragraph 1(c) (hereinafter, “Computers”¹), including:

- a. evidence of the times the Computers were used in furtherance of the Subject Offenses;
- b. passwords, encryption keys, and other access devices that may be necessary to access the Computers;
- c. documentation and manuals that may be necessary to access the Computers or to conduct a forensic examination of the Computers;
- d. evidence of software that would allow others to control the Computers, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- e. evidence indicating how and when the Computers were accessed or used in furtherance of the Subject Offenses;
- f. evidence indicating the Computers’ user’s/users’ state of mind as it relates to the Subject Offenses;
- g. evidence of the attachment to the Computers of other storage devices or similar containers for electronic evidence in furtherance of the Subject Offenses;
- h. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Computers;
- i. records of or information about Internet Protocol addresses used by the Computers;
- j. records of or information about the Computers’ Internet activity, and Internet activity of other electronic devices via use of wifi networks available on the Subject Premises, in furtherance of the Subject Offenses, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

¹ The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

3. Records of telephone calls or other communications in furtherance of each of the Subject Offenses to or from employees assigned to or using workstation number 173 on the 16th floor of the Subject Premises from of November 14, 2016 through March 16, 2017.

4. In addition, with respect to the CP offenses, such items shall also specifically include:

- a. Evidence of computer programs used to access, transmit, or store information relating to the CP Offenses;
- b. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from computer devices, storage media, and related electronic equipment;
- c. Evidence of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
- d. Motion pictures, films, videos, and other recordings of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
- e. Correspondence and records pertaining to violation of the CP Offenses including, but not limited to electronic mail, chat logs, electronic messages, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions involving any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
- f. Records or other items which evidence ownership, control, or use of, or access to computer devices, storage media, and related electronic equipment used to access, transmit, or store information relating to the CP Offenses, including but not limited to sales receipts, warranties, bills for internet access, registry entries, configuration files, saved usernames and passwords, user profiles, email contacts, and photographs.
- g. Information or correspondence pertaining to affiliation with any child exploitation bulletin boards, chat forums, or organizations;
- h. Any child pornography as defined by 18 U.S.C. § 2256(8);
- i. Any child erotica, defined as suggestive visual depictions of nude minors which do not constitute child pornography as defined by 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined by 18 U.S.C. § 2256(2);

- j. Notes, documents, records, invoices, or correspondence, in any format and medium, including, but not limited to, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);
- k. Names, and lists of names and addresses of individuals (including minors) related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);
- l. Mailing lists and/or supplier lists related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2); and
- m. Financial records, including credit card information, bills, and payment records related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

5. In addition, with respect to the Copyright Offenses, such items shall also specifically include:

- a. Evidence of computer programs used to transmit or store information relating to the Copyright Offenses;
- b. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from computer devices, storage media, and related electronic equipment;
- c. Evidence of copyrighted works, including motion pictures, films, videos, other recordings, and documents relating to the Copyright Offenses;
- d. Correspondence and records pertaining to violation of the Copyright Offenses including, but not limited to electronic mail, chat logs, electronic messages, and records bearing on the transmission, receipt, and/or storage of copyrighted works;
- e. Records or other items which evidence ownership, control, or use of, or access to computer devices, storage media, and related electronic equipment used to transmit or store information relating to the Copyright Offenses, including but not limited to sales receipts, warranties, bills for internet access, registry

entries, configuration files, saved usernames and passwords, user profiles, email contacts, and photographs.

- f. Any copyrighted works;
- g. Notes, documents, records, invoices, or correspondence, in any format and medium, including, but not limited to, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, related to the transmission, receipt, and/or storage of copyrighted works;
- h. Names, and lists of names and addresses of individuals (including minors) related to the transmission, receipt, and/or storage of copyrighted works;
- i. Mailing lists and/or supplier lists related to the transmission, receipt, and/or storage of copyrighted works; and
- j. Financial records, including credit card information, bills, and payment records related to the transmission, receipt, and/or storage of copyrighted works.

B. Search and Seizure of Electronically Stored Information

The items to be searched and seized from the Subject Premises also include any computer devices and storage media that may contain any electronically stored information falling within the categories set forth in Section II.A of this Attachment above, including, but not limited to, desktop and laptop computers, disk drives, modems, thumb drives, personal digital assistants, smart phones, digital cameras, and scanners. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

The items to be searched and seized from the Subject Premises also include:

- 1. Any items or records needed to access the data stored on any seized or copied computer devices or storage media, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.
- 2. Any items or records that may facilitate a forensic examination of the computer devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.

3. Any evidence concerning the persons with access to, control over, or ownership of the seized or copied computer devices or storage media.

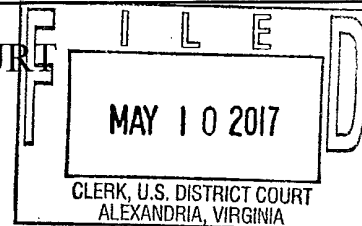
C. Review of ESI

Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques, including but not limited to:

- surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few "pages" of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files;
- scanning storage areas for deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- making reasonable efforts to utilize computer search methodology to search only for files, documents, or other electronically stored information within the categories identified in Sections II.A and II.B of this Attachment.

UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

In the Matter of the Search of
*(Briefly describe the property to be searched
 or identify the person by name and address)*
 Electronic Devices Previously Seized from the
 Premises of 200 East 39th Street, Apartment 8C,
 New York, NY 10016

Case No. 1:17-SW-243

UNDER SEAL

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Electronic devices located at a U.S. Government facility in Herndon, Virginia,

located in the Eastern District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT A

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
 18 U.S.C. 2252
 18 U.S.C. 2252A
 17/18 U.S.C. 506/2319

Offense Description
 Possession and production of sexually explicit material relating to children;
 Activities relating to material containing child pornography;
 Criminal infringement of a copyright

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☒ Continued on the attached sheet.
☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA/SAUSA:

AUSA Neil Hammerstrom

Applicant's signature

Garrett L. Igo, FBI Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 05/10/2017

/s/
 Michael S. Nachmanoff
 United States Magistrate Judge

Judge's signature

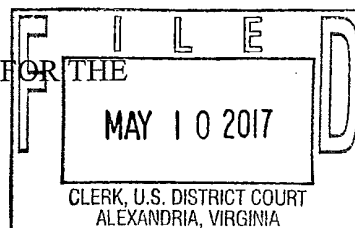
City and state: Alexandria, Virginia

Michael S. Nachmanoff, United States Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN THE MATTER OF THE SEARCH OF:)
Electronic Devices Previously Seized from the)
Premises of 200 East 39th Street, Apartment 8C,)
New York, NY 10016)

UNDER SEAL

Case No. 1:17-SW-243

AFFIDAVIT IN SUPPORT OF A SEARCH AND SEIZURE WARRANT

I, Garrett L. Igo, being duly sworn, hereby deposes and says:

I. Introduction

A. Affiant

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI") assigned to the New York Field Office, and I have been so employed by the FBI since 2011. I am currently assigned to a squad responsible for counterespionage matters and have worked in the field of counterintelligence from 2011 to present. In the course of my duties as a Special Agent, I am responsible for investigating offenses involving espionage and related violations of law, including unauthorized retention, gathering, transmitting or losing classified documents or materials; unauthorized removal and retention of classified documents or materials; illegally acting in the United States as a foreign agent; other national security offenses; and the making of false statements. As a result of my involvement in espionage investigations and investigations involving the unauthorized disclosure or retention of classified information, as well as my training in counterintelligence operations, I am familiar with the tactics, methods, and techniques of United States persons who possess, or have possessed a United States Government security clearance and may choose to harm the United States by misusing their access to classified information. I am also

familiar, though my training and experience, with the use of computers in criminal activity and the forensic analysis of electronically stored information.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the electronic devices specified below (“Subject Devices”) for the items and information described in Attachment A. Specifically, and as discussed in detail below, the Subject Devices were previously seized and searched pursuant to a separate warrant defined herein as the “Schulte Search Warrant,” and which was issued in connection with an investigation into the unlawful dissemination of classified materials.

3. While searching the Subject Devices for evidence, fruits, and instrumentalities of the offenses set forth in the Schulte Search Warrant, law enforcement officers encountered what appears to be an image of child pornography on one of the Subject Devices. Upon discovery of this suspected image of child pornography, the FBI promptly contacted the Assistant United States Attorneys involved in this investigation to inform them of this development, and the decision was made to seek additional authorization under Rule 41 of the Federal Rules of Criminal Procedure to search the Subject Devices for evidence, fruits, and instrumentalities of offenses involving child pornography, as specified below.

4. Similarly, while searching the Subject Devices for evidence, fruits, and instrumentalities of the offenses set forth in the Schulte Search Warrant, law enforcement officers also encountered what appears to be evidence of copyright infringement—specifically, the illegal streaming of dozens of movies—on one of the Subject Devices. Upon discovery of this evidence, the FBI also promptly contacted the Assistant United States Attorneys involved in this investigation to inform them of this development, and the decision was made to seek additional authorization under Rule 41 of the Federal Rules of Criminal Procedure to search the Subject

Devices for evidence, fruits, and instrumentalities of offenses involving copyright infringement, as specified below.

5. This Affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information (“ESI”). Because this Affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. The Subject Offenses

6. For the reasons detailed below, I believe that there is probable cause to believe that the Subject Devices also contain evidence, fruits, and instrumentalities of (i) violations of Title 18, United States Code, Section 2252 (possession, transportation, receipt, distribution, production, and reproduction of sexually explicit material relating to children) and Title 18, United States Code, Section 2252A (activities relating to material constituting or containing child pornography) (the “CP Offenses”); and (ii) violations of Title 17, United States Code, Section 506 and Title 18, United States Code, Section 2319 (criminal infringement of a copyright) (the “Copyright Offenses”).

C. Terminology

7. The term “computer,” as used herein, is defined as set forth in Title 18, United States Code, Section 1030(e)(1).

8. The terms “records,” “documents,” and “materials” include all information recorded in any form, visual or oral, and by any means, whether in handmade form (including, but

not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical discs, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device), as well as the equipment needed to record such information (including but not limited to cameras and video recording and storage devices).

9. The term child pornography is defined in Title 18, United States Code, Section 2256(8) in pertinent part as “any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where . . . the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct.”¹

10. The terms “Minor,” “Sexually Explicit Conduct” and “Visual Depiction” are defined as set forth in Title 18, United States Code, Section 2256.

II. Probable Cause Justifying Search of the Subject Devices

A. Probable Cause for Evidence of CP Offenses

11. On March 13, 2017, the Honorable Barbara C. Moses, a U.S. Magistrate Judge for the Southern District of New York, issued a search warrant (the “Schulte Search Warrant”) to

¹ See also *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002) (analyzing constitutional validity of the definitions set forth in 18 U.S.C. § 2256(8)).

search the residence of JOSHUA ADAM SCHULTE located at 200 East 39th Street, Apartment 8C, New York, New York 10016 (the “Residence”).² The Schulte Search Warrant was issued in connection with the investigation of the unauthorized dissemination on March 7, 2017, by wikileaks.org of documents and files that contained classified, national defense information belonging to the Central Intelligence Agency (the “Classified Materials”). As a result, the Schulte Search Warrant authorized the search of the Premises and any electronic devices found therein, for evidence, fruits, and instrumentalities of offenses relating to the unauthorized disclosure of the Classified Materials (the “Espionage Offenses”).

12. On or about March 15, 2017, members of the FBI searched the Residence.³ During the course of that search, law enforcement officers recovered, among other things, the Subject Devices, including multiple computers, servers, and other portable electronic storage devices.⁴ Following the seizure of the Subject Devices, the devices were transported by the FBI for analysis and examination to a U.S. Government facility in Herndon, Virginia, within the Eastern District of Virginia, where they remain as of the date of this application.

13. Based on my conversations with members of the FBI who are involved in searching the Subject Devices for evidence, fruits, and instrumentalities of the Espionage Offenses pursuant to the terms of the Schulte Search Warrant, I have learned, among other things, that on or about April 7, 2017, a photograph was discovered on SCHULTE’s desktop computer (the “Desktop

² A copy of the Schulte Search Warrant is attached as Exhibit A. A copy of the Affidavit in support of the Schulte Search Warrant is attached as Exhibit B and is incorporated herein by reference.

³ The March 15, 2017 search of the Residence was pursuant to a second search warrant issued by the Honorable Barbara C. Moses on the same day as the search. The Government sought a second search warrant because the Schulte Search Warrant was executed covertly on or about March 14, 2017. However, the items to be searched and seized pursuant to the second search warrant were identical to that which is set forth in the Schulte Search Warrant attached to this Affidavit.

⁴ A list of the Subject Devices is attached as Exhibit C.

Computer”) that appears to depict child pornography (the “CP Picture”). The Desktop Computer appears to have been connected to other Subject Devices in the Residence, including several servers. As a result, data on the Desktop Computer was likely also accessible through, or available on, some of the other Subject Devices in the Residence.

14. Based on my conversations with FBI agents who have spoken to an agent who is assigned to the Crimes Against Children Squad (the “CACS Agent”) and who has reviewed the CP Picture, I understand that the CP Picture appears to depict child pornography.⁵ Specifically, the CACS Agent believes the CP Picture depicts a naked young child on all fours and what appear to be two adults around her, one of whom appears to be performing a sexual act on the child—oral sex around the child’s buttocks. The CACS Agent also believes that the child is a minor based on, among other things, body structure, lack of breast development, and lack of pubic hair.⁶

⁵ Based on my conversations with the CACS Agent, I understand that it is possible that the CP Picture (like many photographs of child pornography) could be altered and not a real picture. However, the CACS Agent had only reviewed a printout of the CP Picture. Members of the FBI who analyzed the Desktop Computer have informed me that the CP Picture looks more like an actual photo when viewed on the computer as opposed to when printed. I know that an agent involved in this investigation has viewed the CP Picture on the Desktop Computer and concluded that it is an actual photograph.

⁶ On or about April 14, 2017, the Honorable Theresa C. Buchanan, United States Magistrate Judge, Eastern District of Virginia, issued a search warrant (the “April 14 Search Warrant”) identical in part to that sought here, *i.e.*, expanding the scope of the search of the Subject Devices to include evidence, fruits, and instrumentalities of the CP Offenses. The April 14 Search Warrant also expanded the search of the Subject Devices to include evidence, fruits, and instrumentalities of the Copyright Offenses. The probable cause set forth in support of the April 14 Search Warrant—as it related to the CP Offenses only (*i.e.*, not the Copyright Offenses)—relied in part on evidence obtained from the results of a prior search warrant issued on or about March 14, 2017 in the Southern District of New York pursuant to the Stored Communications Act, 18 U.S.C. § 2703 (the “SCA Search Warrant”). I have recently learned that, although the SCA Search Warrant limited the scope of that search to evidence, fruits, and instrumentalities of the Espionage Offenses, while executing that search, agents also conducted a limited search for evidence relating to child pornography, and such evidence was used in support of the April 14 Search Warrant application to expand the search of the Subject Devices to include evidence, fruits, and instrumentalities of the CP Offenses. The limited search related to child pornography occurred after prosecutors made

15. Based on my training, experience, and discussions with other FBI agents, I know that persons who collect and distribute child pornography frequently collect and view sexually explicit materials in a variety of media, such as photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media that they use for their own sexual arousal and gratification. These examples of visual media containing sexually explicit materials are often times stored on various devices, such as the Subject Devices, including but not limited to, computers, disk drives, servers, modems, thumb drives, personal digital assistants, mobile phones and smart phones, digital cameras, and scanners, and the data within the aforesaid objects relating to said materials.

16. In addition, I know that individuals who collect and distribute child pornography, in the event that they change computers, will often back up or transfer files from their old computers' hard drives to that of their new computers, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity. In addition, individuals who engage in such criminal activity will often also store or transfer files on electronic storage media other than computer hard drives, including thumb drives, flash memory cards, CD-ROMs, or portable hard drives to, for example, facilitate the use of the information or to transfer it to co-conspirators in support of the criminal scheme.

the decision to obtain a new, expanded search warrant based upon the April 7, 2017 discovery of suspected child pornography on the Desktop Computer, described above. Although I believe that there was ample probable cause set forth in the April 14 Warrant application—separate and apart from the limited evidence obtained from the SCA Search Warrant cited therein—to justify an expanded search of the Subject Devices for evidence, fruits and instrumentalities of the CP Offenses, out of an abundance of caution, and because the search of the Subject Devices (which consists of numerous terabytes of data) is only partially complete, I am submitting this renewed application, which does not rely in any way on the evidence obtained from the SCA Warrant. In the interim, agents have been instructed by the Assistant United States Attorneys involved in this investigation to stop any searches related to the CP Offenses absent renewed additional authorization under Rule 41 of the Federal Rules of Criminal Procedure.

17. I also know that the child pornography detailed above was likely downloaded via the Internet using the Desktop Computer or other of the Subject Devices. As a result, the Desktop Computer and other Subject Devices may contain messages, emails, photographs, and/or videos relating to the possession, receipt, or production of child pornography. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files can be stored on a hard drive for years at little or no cost. Even when such files have been deleted, they can often be recovered, depending on how the hard drive has subsequently been used, months or years later with forensics tools. Specifically, when a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Deleted files, or remnants of deleted files, may accordingly reside in “slack space” (space that is not being used for storage of a file) for long periods of time before they are overwritten. In addition, a computer’s operating system may keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are generally automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve from a hard drive or other electronic storage media depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits.

18. Based on the foregoing, I respectfully submit there is probable cause to believe that JOSHUA ADAM SCHULTE has engaged in the CP Offenses, and that evidence of this criminal activity is likely to be found on the Subject Devices. As a result, I am seeking authorization for a

search warrant to search the Subject Devices for evidence of the CP Offenses. This includes, as set forth in Attachment A, the following:

- Evidence of computer programs used to access, transmit, or store information relating to the CP Offenses;
- Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from computer devices, storage media, and related electronic equipment;
- Evidence of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
- Motion pictures, films, videos, and other recordings of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
- Correspondence and records pertaining to violation of the CP Offenses including, but not limited to electronic mail, chat logs, electronic messages, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions involving any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
- Records or other items which evidence ownership, control, or use of, or access to computer devices, storage media, and related electronic equipment used to access, transmit, or store information relating to the CP Offenses, including but not limited to sales receipts, warranties, bills for internet access, registry entries, configuration files, saved usernames and passwords, user profiles, email contacts, and photographs.
- Information or correspondence pertaining to affiliation with any child exploitation bulletin boards, chat forums, or organizations;
- Any child pornography as defined by 18 U.S.C. § 2256(8);
- Any child erotica, defined as suggestive visual depictions of nude minors which do not constitute child pornography as defined by 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined by 18 U.S.C. § 2256(2);
- Notes, documents, records, invoices, or correspondence, in any format and medium, including, but not limited to, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);
- Names, and lists of names and addresses of individuals (including minors) related to the possession, distribution, receipt, or production of, or access with intent to view, child

pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);

- Mailing lists and/or supplier lists related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2); and
- Financial records, including credit card information, bills, and payment records related to related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2)

19. This application also requests authorization to search the ESI on the Subject Devices pursuant to the same procedures as set forth in the Schulte Search Warrant. (*See* Schulte Search Warrant Application, Part IV.)

B. Probable Cause for Evidence of Copyright Offenses

20. Based on my conversations with members of the FBI who are involved in searching the Subject Devices for evidence, fruits, and instrumentalities of the Espionage Offenses pursuant to the terms of the Schulte Search Warrant, I have learned, among other things, that at least one of the servers recovered from the Residence (“Server-1”) has indications that SCHULTE was involved in illegally sharing copyrighted movies over the Internet. Specifically, Server-1’s command log (which shows the history of commands sent to Server-1 by the user, likely via a computer connected to Server-1), indicates that SCHULTE participated in the sharing of dozens of movies using “torrent trackers.”⁷ Based on my training, experience and conversations with others, I understand that torrent trackers are computer code (or a “protocol”) that connects

⁷ Upon viewing the command log, which was searched pursuant to the terms of the Schulte Search Warrant for evidence regarding the Espionage Offenses, and upon seeing indications of illegal movie sharing, members of the FBI stopped viewing the command log and contacted the U.S. Attorney’s Office.

computers on the Internet to each other in order to facilitate the transfer of large files over the Internet.

21. Based on my training, experience, and my review of the public catalog of copyrighted works available through the United States Copyright Office, I know that most, if not all, of the movies that SCHULTE appears to have participated in sharing are copyrighted works registered with the United States Copyright Office. For example, among the many movies that were apparently shared include *Hacksaw Ridge*; *The Revenant*; *Captain America: Civil War*; and *The Hateful Eight*, all of which are copyrighted works currently registered with the United States Copyright Office.

22. In or about March 2017, FBI agents conducted interviews of multiple CIA employees who know SCHULTE. Among other things, one of those employees stated that SCHULTE operates a service allowing users to stream movies over the internet (the “Streaming Service”) and that SCHULTE manages the accounts of users of the Streaming Service.

23. Based on my review of a telephone that was among the Subject Devices for evidence, fruits, and instrumentalities of the Espionage Offenses pursuant to the terms of the Schulte Search Warrant, I have learned, among other things, that on or about October 31, 2016, SCHULTE sent an email to approximately 20 other individuals with the subject line “Pedbsktbl1 Plex Server Downtime 11/9/2016-1/2017” (the “Email”). In the Email, SCHULTE notifies the recipients that the “server will be down as it relocates to NYC starting 11/9. Thus, you will have the next 9 days to select and download material you may wish to watch during that downtime. Hopefully, the server will be back and running mid to late December – January at the latest.” Based on my training, experience, and participation in this investigation, I believe that SCHULTE

was referring to the Streaming Service and was alerting users that the service would be unavailable while he moved to New York in late 2016.

24. Based on my training, experience, and discussions with other FBI agents, I know that persons who engage in the illegal transmission, distribution, and receipt of copyrighted works typically store evidence of such works on various devices, such as the Subject Devices, including but not limited to, computers, disk drives, servers, modems, thumb drives, personal digital assistants, mobile phones and smart phones, digital cameras, and scanners, and the data within the aforesaid objects relating to said materials.

25. In addition, I know that individuals who engage in the illegal distribution of copyrighted works, in the event that they change computers, will often back up or transfer files from their old computers' hard drives to that of their new computers, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity. Furthermore, individuals who engage in such criminal activity will often also store or transfer files on electronic storage media other than computer hard drives, including thumb drives, flash memory cards, CD-ROMs, or portable hard drives to, for example, facilitate the use of the information or to transfer it to co-conspirators in support of the criminal scheme.

26. I also know that the movies detailed above were likely downloaded via the Internet using Server-1 and other of the Subject Devices. As a result, Server-1 and other Subject Devices may contain messages, emails, and/or videos relating to the transmission, distribution, and receipt of copyrighted works. As noted above, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet.

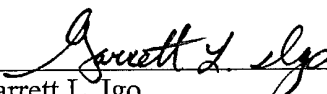
27. Based on the foregoing, I respectfully submit there is also probable cause to believe that JOSHUA ADAM SCHULTE has engaged in the Copyright Offenses, and that evidence of this criminal activity is likely to be found on the Subject Devices. I am also seeking authorization for a search warrant to search the Subject Devices for evidence of the Copyright Offenses. Specifically, this includes, as set forth in Attachment A, the following:

- Evidence of computer programs used to transmit or store information relating to the Copyright Offenses;
- Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from computer devices, storage media, and related electronic equipment;
- Evidence of copyrighted works, including motion pictures, films, videos, other recordings, and documents relating to the Copyright Offenses;
- Correspondence and records pertaining to violation of the Copyright Offenses including, but not limited to electronic mail, chat logs, electronic messages, and records bearing on the transmission, receipt, and/or storage of copyrighted works;
- Records or other items which evidence ownership, control, or use of, or access to computer devices, storage media, and related electronic equipment used to transmit or store information relating to the Copyright Offenses, including but not limited to sales receipts, warranties, bills for internet access, registry entries, configuration files, saved usernames and passwords, user profiles, email contacts, and photographs.
- Any copyrighted works;
- Notes, documents, records, invoices, or correspondence, in any format and medium, including, but not limited to, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, related to the transmission, receipt, and/or storage of copyrighted works;
- Names, and lists of names and addresses of individuals (including minors) related to the transmission, receipt, and/or storage of copyrighted works;
- Mailing lists and/or supplier lists related to the transmission, receipt, and/or storage of copyrighted works; and
- Financial records, including credit card information, bills, and payment records related to the transmission, receipt, and/or storage of copyrighted works.

28. This application also requests authorization to search the ESI on the Subject Devices pursuant to the same procedures as set forth in the Schulte Search Warrant. (*See* Schulte Search Warrant Application, Part IV.)


III. Conclusion and Ancillary Provisions

29. Based on the foregoing, I respectfully request the court to issue a warrant to search the items and information specified in Attachment A to this Affidavit and to the Search and Seizure Warrant. In light of the confidential nature of the continuing investigation, I respectfully request that this Affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise.



Garrett L. Igo
Special Agent
Federal Bureau of Investigation

Sworn to and signed before me on
this 10th day of May 2017

_____/s/ 
Michael S. Nachmanoff
United States Magistrate Judge

Michael S. Nachmanoff
United States Magistrate Judge

Attachment A

I. Devices to be Searched—Subject Devices

The devices to be searched (the “Subject Devices”) include any and all electronic devices seized pursuant to a search warrant executed on or about March 15, 2017 at the premises described as apartment 8C in a building located at 200 East 39th Street, New York, New York 10016.

II. The Search of the Subject Devices

A. Evidence, Fruits, and Instrumentalities of the Child Pornography Offenses

The Subject Devices may be searched for the following evidence, fruits, and/or instrumentalities of violations of Title 18, United States Code, Sections 2252 (activities relating to material constituting or containing child pornography) and 2252A (possession, transportation, receipt, distribution, production, and reproduction of sexually explicit material relating to children) (the “CP Offenses”):

- Evidence of computer programs used to access, transmit, or store information relating to the CP Offenses;
- Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from computer devices, storage media, and related electronic equipment;
- Evidence of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
- Motion pictures, films, videos, and other recordings of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
- Correspondence and records pertaining to violation of the CP Offenses including, but not limited to electronic mail, chat logs, electronic messages, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions involving any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
- Records or other items which evidence ownership, control, or use of, or access to computer devices, storage media, and related electronic equipment used to access, transmit, or store information relating to the CP Offenses, including but not limited to sales receipts, warranties, bills for internet access, registry entries, configuration files, saved usernames and passwords, user profiles, email contacts, and photographs.

- Information or correspondence pertaining to affiliation with any child exploitation bulletin boards, chat forums, or organizations;
- Any child pornography as defined by 18 U.S.C. § 2256(8);
- Any child erotica, defined as suggestive visual depictions of nude minors which do not constitute child pornography as defined by 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined by 18 U.S.C. § 2256(2);
- Notes, documents, records, invoices, or correspondence, in any format and medium, including, but not limited to, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);
- Names, and lists of names and addresses of individuals (including minors) related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);
- Mailing lists and/or supplier lists related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2); and
- Financial records, including credit card information, bills, and payment records related to related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

B. Evidence, Fruits, and Instrumentalities of the Copyright Offenses

The Subject Devices may also be searched for the following evidence, fruits, and/or instrumentalities of violations of violations of 17 U.S.C. § 506 and 18 U.S.C. § 2319 (criminal infringement of a copyright) (the “Copyright Offenses”):

- Evidence of computer programs used to transmit or store information relating to the Copyright Offenses;
- Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from computer devices, storage media, and related electronic equipment;

- Evidence of copyrighted works, including motion pictures, films, videos, other recordings, and documents relating to the Copyright Offenses;
- Correspondence and records pertaining to violation of the Copyright Offenses including, but not limited to electronic mail, chat logs, electronic messages, and records bearing on the transmission, receipt, and/or storage of copyrighted works;
- Records or other items which evidence ownership, control, or use of, or access to computer devices, storage media, and related electronic equipment used to transmit or store information relating to the Copyright Offenses, including but not limited to sales receipts, warranties, bills for internet access, registry entries, configuration files, saved usernames and passwords, user profiles, email contacts, and photographs.
- Any copyrighted works;
- Notes, documents, records, invoices, or correspondence, in any format and medium, including, but not limited to, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, related to the transmission, receipt, and/or storage of copyrighted works;
- Names, and lists of names and addresses of individuals (including minors) related to the transmission, receipt, and/or storage of copyrighted works;
- Mailing lists and/or supplier lists related to the transmission, receipt, and/or storage of copyrighted works; and
- Financial records, including credit card information, bills, and payment records related to the transmission, receipt, and/or storage of copyrighted works.

C. Review of ESI

In conducting a review of ESI on the Subject Devices, law enforcement personnel may use various techniques, including but not limited to:

- surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files;
- scanning storage areas for deliberately hidden files;

- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- making reasonable efforts to utilize computer search methodology to search only for files, documents, or other electronically stored information within the categories identified in Section II.A of this Attachment.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Section II.A and II.B. of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all ESI from the Subject Devices if necessary to evaluate its contents and to locate all data responsive to the warrant.

EXHIBIT A

AO 93 (SDNY Rev. 01/17) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
Southern District of New YorkIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)200 East 39th Street, Apartment 8C, New York, New
York 10016, as well as Any Closed Containers/Items;
See Attachment A

Case No.

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Southern District of New York
(identify the person or describe the property to be searched and give its location):

200 East 39th Street, Apartment 8C, New York, New York 10016; see Attachment A

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property
to be seized):

See Attachment A

The search and seizure are related to violation(s) of (insert statutory citations):

18 U.S.C. 793(d), 793(e), 1030(a)(1), 1030(a)(2)(B).

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or
property.**YOU ARE COMMANDED** to execute this warrant on or before March 27, 2017

(not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10 p.m.☒ at any time in the day or night as I find reasonable cause has been
established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property
taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the
place where the property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an
inventory as required by law and promptly return this warrant and inventory to the Clerk of the Court.☒ Upon its return, this warrant and inventory should be filed under seal by the Clerk of the Court. SJM
USMJ Initials☒ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay
of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be
searched or seized (check the appropriate box) ☒ for 30 days (not to exceed 30).☐ until, the facts justifying, the later specific date of _____.S/Barbara MosesDate and time issued: MAR 13 2017 1:07

Judge's signature

City and state: New York, NY

Honorable Barbara C. Moses

Printed name and title

JAS_027255

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
-----------	---------------------------------	--

Inventory of the property taken and name of any person(s) seized:

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the Court.

Date: _____

Executing officer's signature

Printed name and title

Attachment A

I. Premises to be Searched—Subject Premises

The premises to be searched (the “Subject Premises”) is described as follows, and includes all locked and closed containers found therein:

The Subject Premises is particularly described as apartment 8C in a building located at 200 East 39th Street, New York, New York 10016 (the “Building”). The Building is located near the corner of 39th Street and Third Avenue. The Building is nineteen stories high and contains approximately ninety-one apartment units. The Subject Premises is a one-bedroom apartment located on the eighth floor of the Building, and it is clearly identifiable as apartment 8C from the outside of the Subject Premises.

II. Execution of the Warrant

Law enforcement agents are permitted to execute the search warrant at any time in the day or night, and further to execute the search warrant covertly without advance or contemporaneous notice of the execution of the search warrant. Law enforcement agents will provide notice of the execution of the warrant within seven days of execution unless there is a new showing, made to the Court, that delayed notice is appropriate.

III. Items to Be Searched and Seized

A. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be searched and/or seized from the Subject Premises include the following evidence, fruits, and instrumentalities of: (i) the unauthorized possession and, *inter alia*, the communication of national defense information to someone not entitled to receive it, in violation of Title 18, United States Code, Section 793(d); (ii) the unlawful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); (iii) exceeding authorized access to a computer in order to obtain national defense information with reason to believe that information could be used to the injury of the United States and the advantage of a foreign nation and willfully transmitting that information to a person not entitled to receive it, in violation of Title

18, United States Code, Section 1030(a)(1); and (iv) intentionally exceeding authorized access and thereby obtaining information from a department or agency of the United States, in violation of Title 18, United States Code, Section 1030(a)(2)(B) (collectively, the “Subject Offenses”):

1. Evidence concerning occupancy or ownership of the Subject Premises, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys.
2. Evidence concerning the identity or location of, and communications with, any co-conspirators.
3. Any and all notes, documents, records, correspondence, or materials, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, and handwritten notes), pertaining to the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials.
4. Electronic devices (including but not limited to computers, tablets, smartphones, and cellular telephones) and storage media used in furtherance of the Subject Offenses, containing evidence of the Subject Offenses, or containing evidence authorized for seizure in paragraphs 1, 2 and 3 above. The term “storage media” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

5. Electronic forensic evidence relating to the Subject Offenses, including for any electronic device or storage media whose search and/or seizure is authorized by this warrant as described above in paragraph 4 (hereinafter, “Computers”¹), including:

- a. evidence of the times the Computers were used in furtherance of the Subject Offenses;
- b. passwords, encryption keys, and other access devices that may be necessary to access the Computers;
- c. documentation and manuals that may be necessary to access the Computers or to conduct a forensic examination of the Computers;
- d. evidence of software that would allow others to control the Computers, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- e. evidence indicating how and when the Computers were accessed or used in furtherance of the Subject Offenses;
- f. evidence indicating the Computers’ user’s/users’ state of mind as it relates to the Subject Offenses;
- g. evidence of the attachment to the Computers of other storage devices or similar containers for electronic evidence in furtherance of the Subject Offenses;

¹ The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

- h. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Computers;
- i. records of or information about Internet Protocol addresses used by the Computers;
- j. records of or information about the Computers' Internet activity in furtherance of the Subject Offenses, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

6. If law enforcement personnel seize the computer(s) or other electronic device(s), the personnel will search the computer and/or device(s) within a reasonable amount of time, not to exceed 60 days from the date of execution of the warrant. If, after such a search has been conducted, it is determined that a computer or device contains any data listed in paragraphs 1 through 3, the Government will retain the computer or device. If it is determined that the computer(s) or device(s) are no longer necessary to retrieve and preserve the data, and the items are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(b), such materials and/or equipment will be returned within a reasonable time. In any event, such materials and/or equipment shall be returned no later than 60 days from the execution of this warrant, unless further application is made to the Court.

B. Search and Seizure of Electronically Stored Information

The items to be searched and seized from the Subject Premises also include any computer devices and storage media that may contain any electronically stored information falling within the categories set forth in Section III.A of this Attachment above, including, but not limited to,

desktop and laptop computers, disk drives, modems, thumb drives, personal digital assistants, smart phones, digital cameras, and scanners. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

The items to be searched and seized from the Subject Premises also include:

1. Any items or records needed to access the data stored on any seized or copied computer devices or storage media, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.
2. Any items or records that may facilitate a forensic examination of the computer devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.
3. Any evidence concerning the persons with access to, control over, or ownership of the seized or copied computer devices or storage media.

C. Review of ESI

Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques, including but not limited to:

- surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few "pages" of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files;
- scanning storage areas for deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- making reasonable efforts to utilize computer search methodology to search only for files, documents, or other electronically stored information within the categories identified in Sections I.A and I.B of this Attachment.

EXHIBIT B

UNITED STATES DISTRICT COURT

for the
Southern District of New York

17 MAG 1856

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Case No.

200 East 39th Street, Apartment 8C, New York, New
York 10016, as well as Any Closed Containers/Items

APPLICATION FOR A SEARCH AND SEIZURE WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

200 East 39th Street, Apartment 8C, New York, New York 10016

located in the Southern District of New York, there is now concealed (identify the person or describe the property to be seized):

See Attached Affidavit and its Attachment A

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section(s)

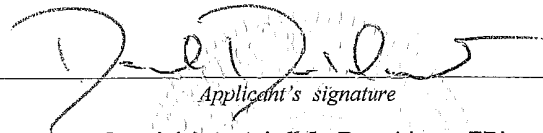
Offense Description(s)

18 U.S.C. 793(d), 793(e), Offenses relating to unauthorized possession and distribution of
 1030(a)(1), 1030(a)(2)(B). national defense information

The application is based on these facts:

See Attached Affidavit and its Attachment A

- ☒ Continued on the attached sheet.
☒ Delayed notice of 30 days (give exact ending date if more than 30 days:) is requested
 under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Special Agent Jeff D. Donaldson, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 03/13/2017

City and state: New York, NY

S/Barbara Moses

Judge's signature

Honorable Barbara C. Moses

Printed name and title

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of the Application of the United States of America for a Search Warrant for the Premises Known and Described as 200 East 39th Street, Apartment 8C, New York, New York 10016, as well as Any Closed Containers/Items Contained in the Premises

TO BE FILED UNDER SEAL

**Agent Affidavit in Support of
Application for Search Warrant**

SOUTHERN DISTRICT OF NEW YORK) ss.:

JEFF D. DONALDSON, being duly sworn, deposes and says:

I. Introduction

A. Affiant

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI") assigned to the New York Field Office, and have been employed by the FBI since 2010. I am currently assigned to a squad responsible for counterespionage matters and have worked in the field of counterintelligence from 2010 to present. In the course of my duties as a Special Agent, I am responsible for investigating offenses involving espionage and related violations of law, including unauthorized retention, gathering, transmitting or losing classified documents or materials; unauthorized removal and retention of classified documents or materials; illegally acting in the United States as a foreign agent; other national security offenses; and the making of false statements. As a result of my involvement in espionage investigations and investigations involving the unauthorized disclosure or retention of classified information, as well as my training in counterintelligence operations, I am familiar with the tactics, methods, and techniques of United States persons who possess, or have possessed a United States Government security clearance and may choose to harm the United States by misusing their access to classified information. I am also

familiar, though my training and experience with the use of computers in criminal activity and the forensic analysis of electronically stored information.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises specified below (“Subject Premises”) for the items and information described in Attachment A. This Affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information (“ESI”). Because this Affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. The Subject Premises

3. The Subject Premises is particularly described as apartment 8C in a residential apartment building located at 200 East 39th Street, New York, New York 10016 (the “Building”). The Building is located near the corner of 39th Street and Third Avenue in Manhattan. The Building is nineteen stories high and contains approximately ninety-one apartment units. The Subject Premises is a one-bedroom apartment located on the eighth floor of the Building, and it is clearly identifiable as Apartment 8C from the outside of the Subject Premises.

C. The Subject Offenses

4. For the reasons detailed below, I believe that there is probable cause to believe that the Subject Premises contain evidence, fruits, and instrumentalities of (i) the unauthorized possession and, *inter alia*, the communication of national defense information to someone not entitled to receive it, in violation of Title 18, United States Code, Section 793(d); (ii) the unlawful

retention of national defense information, in violation of Title 18, United States Code, Section 793(e); (iii) exceeding authorized access to a computer in order to obtain national defense information with reason to believe that information could be used to the injury of the United States and the advantage of a foreign nation and willfully transmitting that information to a person not entitled to receive it, in violation of Title 18, United States Code, Section 1030(a)(1); and (iv) intentionally exceeding authorized access to a computer and thereby obtaining information from a department or agency of the United States, in violation of Title 18, United States Code, Section 1030(a)(2)(B) (collectively the “Subject Offenses”).

D. Terminology

5. The term “computer,” as used herein, is defined as set forth in 18 U.S.C. § 1030(e)(1).

6. The terms “records,” “documents,” and “materials” include all information recorded in any form, visual or oral, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical discs, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device), as well as the equipment needed to record such information (including but not limited to cameras and video recording and storage devices).

II. Probable Cause

A. WikiLeaks Publication of Classified CIA Information

7. Based on my review of publicly available material on the Internet, including on the website wikileaks.org (“WikiLeaks”), I know that, on March 7, 2017, WikiLeaks published what it claimed were more than 8,000 documents and files that contained classified information (the “Classified Information”) belonging to the Central Intelligence Agency (“CIA”). In its press release accompanying the Classified Information, WikiLeaks further claimed that:

a. The public dissemination of the Classified Information was “the largest ever” unauthorized publication of classified CIA documents.

b. The Classified Information constituted the “first full part” of a series—thus indicating that there would be subsequent publications of additional sensitive CIA information.

c. The “collection” obtained by WikiLeaks amounted to “more than several hundred million lines of code” and revealed the “entire hacking capacity” of the CIA, including various malware, viruses, and other tools used by the CIA.

8. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that:

a. The information that WikiLeaks claimed was classified CIA information—that is, the Classified Information—was at the time of its disclosure, in fact, classified CIA information.

b. Specifically, the Classified Information was created and maintained by one specific group within the CIA which is responsible for various computer engineering activities, including the development of computer code (the “CIA Group”). That CIA Group exists within a larger CIA component (the “CIA Component”). In March 2016, less than 200 employees were assigned to the CIA Group. And only employees of the CIA Group had access to the computer

network on which the Classified Information that was stolen from the CIA Group's computer network was stored. (Moreover, as described in detail below, only three of those approximately 200 people who worked for the CIA Group had access to the specific portion of the Group's computer network on which the Classified Information was likely stored.)

c. The Classified Information appears to have been stolen from the CIA Component sometime between the night of March 7, 2016 and the night of March 8, 2016.

i. This is based on preliminary analysis of the timestamps associated with the Classified Information which indicates that March 7, 2016 was the latest (or most recent) creation or modification date associated with the Classified Information.

ii. Because, for the reasons described below (*see infra* Part C.10), the Classified Information was apparently copied from an automated daily back-up file, it is likely that the Classified Information was copied either late on March 7, 2016 (after the March 7 nightly back-up was completed) or on March 8, 2016 (before the March 8 nightly back-up was completed).

iii. This is so because if the Classified Information was copied before the March 7 back-up, one would *not* expect to see in the Classified Information documents dated as late as March 7. And if the Classified Information was copied after the March 8 back-up, one *would* expect to see documents dated on or after March 8 because the "back-ups" occur approximately each day.¹

¹ It is of course possible that the Classified Information was copied later than March 8, 2016 even though the creation/modification dates associated with it appear to end on March 7, 2016. For example, the individual who copied and removed the data could have limited his or her copying to data that was modified or created on or before March 7, 2016. (Conversely, however, the Classified Information is unlikely to have been copied before March 7, 2016, because it contains data that was created as recently as March 7, 2016.) Because the most recent timestamp on the Classified Information reflects a date of March 7, 2016, preliminary analysis indicates that the Classified Information was likely copied between the end of the day on March 7 and the end of the day on March 8.

d. The Classified Information was publicly released by WikiLeaks exactly one year to the day (March 7, 2017) from the latest date associated with the Classified Information (March 7, 2016).

e. The duplication and removal from the CIA Group's computer network of the Classified Information and its subsequent public dissemination via WikiLeaks was not authorized by the United States government.

f. The unauthorized disclosure of the Classified Information could—at a minimum—reasonably be expected to cause serious damage to the national security of the United States. *See* Executive Order 13526; 18 C.F.R. § 3a.11(a)(2).

g. The Classified Information is national defense information and its disclosure could reasonably be expected to be used to the injury to the United States and to the advantage of a foreign nation. *See* 18 U.S.C. § 793(d) & (e).

B. The CIA Group's Local Area Computer Network (LAN) and Back-Up Server

9. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that the Classified Information originated in a specific isolated local area computer network ("LAN") used exclusively by the CIA Group.² As described above, in and around March 2016, in total less than 200 people had access to the CIA Group's LAN on which the Classified Information was stored.

a. An isolated network, such as the CIA Group's LAN, is a network-security structure by which the isolated network is physically separated (or "air-gapped") from unsecured networks, such as the public Internet.

² In its press release announcing the publication of the Classified Information, WikiLeaks stated that the Classified Information originated from "an isolated, high-security network."

b. Accordingly, such isolated networks, like the LAN, cannot be accessed from the public Internet, but rather only through those computers which are physically connected to the isolated network.

c. The CIA Group's LAN, and each of its component parts, was maintained in heavily physically secured governmental facilities, which include multiple access controls and various other security measures.

d. The isolated LAN used by the CIA Group was comprised of multiple networked computers and servers. (Each of these component computers and servers were, by definition, inside the electronically isolated LAN.)

i. In order to preserve and protect the CIA Group employees' day-to-day computer engineering work, that work was backed up, on an approximately daily basis, to another server on the CIA Group's LAN that was used to store back-up data (the "Back-Up Server").

ii. Back-ups of the sort stored on the Back-Up Server are designed to ensure that, should the original data be corrupted or deleted, the stored data is not lost, but rather—because of the daily back-ups—is maintained via the daily copies stored on the Back-Up Server.

C. The Publicly Disclosed Classified Information Likely Originated on the CIA Group's Back-Up Server

10. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I understand that the Classified Information that was publicly released by WikiLeaks appears likely to have been copied—specifically—from the CIA Group's Back-Up Server.

a. As described above, the Back-Up Server served as a secondary storage location for data that principally resided on the primary computer network used for CIA Group

employees' day-to-day work writing computer code. Approximately each day, an automated process would back-up that data to the Back-Up Server. Each of those daily back-ups was akin to an electronic "snapshot" of the data on that particular date. In that way, the Back-Up Server simultaneously acquired and stored, on a rolling basis, daily snapshots of the original data.

b. As such, if the data contained on the Back-Up Server was copied *en masse* directly from that Server, the copy would contain numerous iterations (or snapshots) of the similar or same data which had been backed up from the original data, distinguished by date.

c. The publicly released Classified Information does in fact contain numerous iterations (or snapshots) of the similar or same data, distinguished by date.

d. Accordingly, the fact that the Classified Information contains numerous iterations (or snapshots) of the similar or same data, distinguished by date, is strongly supportive of the fact that the Classified Information was taken from the CIA Group's Back-Up Server.³

e. As described above (*see supra* Part II.A.8.c), because the most recent timestamp associated with the Classified Information appears to be March 7, 2016, it is likely that the Classified Information was copied from the Back-Up Server after the daily back-up on March 7, 2016, and before the daily back-up on March 8, 2016.

D. TARGET SUBJECT JOSHUA ADAM SCHULTE Was One of Only Three Employees Across the Entire CIA Who, in March 2016, Had Been Given System Administrator Access To the Back-Up Server

11. Based on my conversations with other law enforcement agents and others, my

³ I understand, based on my conversations with others familiar with the CIA Group's LAN that it would be difficult, if not impossible, to copy from the data (not on the Back-Up Server) the multiple different date-distinguished iterations of the same data that are included in the publicly released Classified Information. In contrast, a single copy of the Back-Up Server would likely include each of the prior iterations (or snapshots) of the same data—which is exactly what is reflected in the publicly released Classified Information.

review of documents, and my training and experience, I know that the CIA Group's LAN was designed such that only those employees who were specifically given a particular type of systems-administrator access ("Systems Administrators") could access the Back-Up Server.

a. Systems Administrators were given a particular username and password in order to log on to and access the Back-Up Server.

b. Conversely, CIA employees who were not designated Systems Administrators were not given access to the Back-Up Server.⁴

12. I know, based on my conversations with other law enforcement agents and others, in approximately March 2016—the month when the Classified Information is assessed to have been copied—only three CIA employees were designated Systems Administrators with access to the CIA Group's Back-Up Server.

a. TARGET SUBJECT JOSHUA ADAM SCHULTE ("SCHULTE") was one of those three Systems Administrators.

i. SCHULTE was employed as a computer engineer by the CIA—specifically in the CIA Group—from in or about May 2010 through on or about November 10, 2016, when he resigned from the CIA.

ii. During SCHULTE's more than six years working in the CIA Group, his responsibilities included, among other things, developing computer code for specific projects, including projects explicitly described in the Classified Information.

⁴ It is, of course, possible that an employee who was not a designated Systems Administrator could find a way to gain access to the Back-Up Server. For example, such an employee could steal and use—without legitimate authorization—the username and password of a designated Systems Administrator. Or an employee lacking Systems Administrator access could, at least theoretically, gain access to the Back-Up Server by finding a "back-door" into the Back-Up Server.

iii. SCHULTE had a skill set that enabled him to write computer code designed to clandestinely copy data from computers.

b. As described above, in March 2016, SCHULTE was one of only three CIA employees throughout the entire CIA who had authorized access to the CIA Group's Back-Up Server from which the Classified Information was likely copied. The publicly released Classified Information published by WikiLeaks, based on a preliminary review, appears to contain the names and/or pseudonyms of, *inter alia*, multiple CIA employees—including two of the three aforementioned individuals with designated Systems Administrator privileges.

i. Names used by the other two CIA Group Systems Administrators were, in fact, published in the publicly released Classified Information.

ii. SCHULTE's name, on the other hand, was not apparently published in the Classified Information.

iii. Thus, SCHULTE was the only one of the three Systems Administrators with access to the Classified Information on the Back-Up Server who was not publicly identified via WikiLeaks's publication of the Classified Information.

c. The other two individuals who served in March 2016 as Systems Administrators for the CIA Group's LAN remain employed by the CIA. SCHULTE resigned from the CIA in November 2016, as described in detail below.

E. SCHULTE Had Access to the Back-Up Server on March 7 and 8, 2016—The Likely Dates of the Copying of the Classified Information

13. As described above (see *supra* Part II.C.10), it appears likely that the Classified Information was copied between March 7 and March 8, 2016.

a. Based on my conversations with other law enforcement agents and others, and my review of documents, including access records of the CIA Component facility in which

SCHULTE worked, I know that he was present at work from approximately:

- i. 10:01 a.m. until 7:16 p.m. on March 7, 2016; and
- ii. 10:19 a.m. until 7:40 p.m. on March 8, 2016.

b. Based on my conversations with other law enforcement agents and others, and my review of documents, I know that on March 8, 2016, the CIA Group held an offsite management retreat for many of its senior and midlevel managers. Accordingly, on March 8th, much of the CIA Group's management, including some to whom SCHULTE reported, were not present in the CIA Component building where SCHULTE and other CIA Group employees worked.

c. I further understand that SCHULTE's workspace (*i.e.*, his desk and computer workstation) was set up such that only three other CIA Group Employees had direct line-of-sight to SCHULTE's desk and computer—that is, only three other employees could see what he was doing at his desk. At least two of those three employees were at the offsite management retreat on March 8, 2016.

d. As described above, in March 2016, only two CIA employees in addition to SCHULTE were designated Systems Administrators with access to the CIA Group's Back-Up Server from which the Classified Information was likely copied. On March 8, 2016, one of those two other designated Systems Administrators was at the offsite management retreat. (The retreat was held at a location that did not have any access to the CIA Group's LAN, including the Back-up Server, and therefore afforded no access to the Classified Information.)⁵

⁵ On March 7 and 8, 2016, the third of the three CIA employees with Systems Administrator access was located at a CIA facility that did, in fact, have access to the Back-Up Server from which the Classified Information was likely copied.

F. SCHULTE's Unauthorized Unilateral Reinstatement of His Own Administrative Privileges

14. Based on my conversations with other law enforcement agents and others, and my review of documents, I understand that, on or about April 4, 2016, around the time of his reassignment to another branch within the CIA Group, many of SCHULTE's administrator privileges on the LAN were revoked, and he was no longer permitted to serve as a Systems Administrator in the CIA Group's LAN.

a. At the same time, on or about April 4, 2016, SCHULTE's computer access to a specific developmental project ("Project-1") was also revoked. Until his reassignment, SCHULTE had been the CIA Group employee with principal responsibility for Project-1.

b. Upon that transfer, principal responsibility for Project-1 was transferred to another CIA Group employee, who received computer access to Project-1.⁶

c. I know from my review of publicly available material on the Internet, including WikiLeaks.org, that Project-1 was one of a small group of CIA projects and capabilities that WikiLeaks highlighted explicitly by name in its March 7, 2017 press release that accompanied the online publication of the Classified Information.

15. Based on my conversations with other law enforcement agents and others, and my review of documents, I understand that, less than two weeks later, on or about April 11, 2016, SCHULTE unilaterally, and without authorization, logged onto the CIA Group's LAN and reinstated his own administrator privileges.

a. On or about April 14, 2016, CIA Group management discovered that

⁶ SCHULTE retained read-only access to Project-1 (but not the ability to alter the code) and the ability to copy the computer code associated with it in order to support another project for which he had responsibility.

SCHULTE had personally re-instituted his administrator privileges without permission.

b. On or about April 18, 2016, SCHULTE received notice regarding CIA policies against personnel restoring their own access to privileges or computer networks after those accesses have been revoked. SCHULTE signed an acknowledgment that he understood that “individuals are not permitted to personally attempt and/or renew their previous authorizations [including administrator privileges] to any particular [computer] system.” That notice further instructed SCHULTE: “do not attempt to restore or provide yourself administrative rights to any project and/or system for which they have been removed.”

c. A little more than one month later, on May 26, 2016, and notwithstanding the warnings described above, SCHULTE made an official request that he again be given full access to Project-1. Before receiving a response to that request, SCHULTE requested access from another employee who, apparently without proper vetting, granted SCHULTE the requested full access to Project-1.

i. On the same day, SCHULTE used that newly obtained access to, unilaterally and without authorization, revoke the computer access permissions of all other CIA Group employees to work on Project-1.

ii. Once this conduct was discovered, SCHULTE was issued a letter of warning that stated, “You were aware of the policy for access and your management’s lack of support for you to retain administrative privileges, but nonetheless you took steps to deliberately violate that policy and gain those privileges.” It continued by warning SCHULTE that any future violations would result in “further administrative action of a more severe nature.”

iii. After receiving the letter of warning, SCHULTE disagreed with some of its conclusions and consequently refused to sign the form.

16. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that the unauthorized duplication, retention and removal of the Classified Information from the CIA Group's computer network, and its placement on the publicly available Internet, exceeds the authorized access to those government-owned and controlled computer networks of any user. *See* 18 U.S.C. § 1030.

G. Internal CIA Investigation of SCHULTE and a CIA Colleague

17. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that, in or around March 2016, SCHULTE came to the attention of CIA security after SCHULTE alleged that another CIA Group co-worker had made a threat against him. SCHULTE expressed deep unhappiness about the way that CIA responded to the alleged threat. He threatened legal action against the CIA for its handling of the situation, and repeatedly stated that he felt that he was being punished by CIA management for reporting the alleged threat incident. SCHULTE informed CIA security that, if "forced into a corner" he would proceed with a lawsuit against the CIA. He also repeatedly threatened that he or his lawyer would go to the media. In addition, CIA security learned that SCHULTE had removed an internal CIA document from CIA facilities that regarded his complaints to the CIA concerning its handling of the alleged threat, despite being told multiple times by CIA security officials not to do so.

18. In approximately August 2016, as part of a standard background reinvestigation of SCHULTE for purposes of renewing his security clearances, the CIA conducted interviews of multiple CIA Group colleagues. Among other things:

a. Some (but not all) colleagues independently reported that SCHULTE's demeanor with his management and colleagues, and his commitment to his work, changed markedly for the worse in or around February 2016.

b. Multiple colleagues stated that SCHULTE had indicated that he felt aggrieved by the CIA in a number of respects. Some also reported that they believed SCHULTE to be untrustworthy and potentially subject to outside coercion. (Other colleagues made no such report and, indeed affirmatively reported that they believed that SCHULTE was, in fact, trustworthy.)

c. Some (but not all) colleagues also reported that SCHULTE's security practices were lax, and that SCHULTE tended not to abide by security guidelines he deemed inconvenient—particularly guidelines concerning when and what kinds of media or data (such as external drives) could be connected or uploaded to CIA computer systems.⁷

H. SCHULTE's November 2016 Resignation from the CIA

19. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that, in connection with and preceding SCHULTE's November 2016 resignation from the CIA, he sent the following communications, among others:

a. Approximately one month prior to his resignation, on October 12, 2016, SCHULTE, using his CIA email account, sent an email to another CIA Group employee at that employee's official email account. The subject line of the email stated, "ROUGH DRAFT of Resignation Letter *EYES ONLY*." The email contained a letter entitled "Letter of Resignation 10/12/16" and addressed to "To whomever it may concern" ("Draft Resignation Letter"). I know from reviewing the Draft Resignation Letter, which spanned approximately three single-spaced pages, the following:

⁷ External drives can be connected to computers and files in order to allow users to move files from the computers onto the portable external drives.

i. SCHULTE began the letter by stating, in substance and in part, that he had “always been a patriot” and would “obviously continue to support and defend this country until the day that I die,” but that “from this day forward” he would “no longer do so as a public servant.”

ii. SCHULTE claimed that he believed that the CIA Group management had unfairly “veiled” CIA leadership from various of SCHULTE’ s previously expressed concerns, including concerns about the network security of the CIA Group’s LAN. SCHULTE continued: “That ends now. From this moment forward you can no longer claim ignorance; you can no longer pretend that you were not involved.”

iii. SCHULTE explained that he was resigning from the CIA because CIA Group management had, among other things, “ignored” issues he had raised about “security concerns” and had attempted to “conceal these practices from senior leadership,” including that the CIA Group’s LAN was “incredibly vulnerable” to the theft of sensitive data. He claimed that one named CIA Group manager had ignored his security concerns and “later attempt[ed] to evade responsibility and blame the decentralized and insecure [CIA Group computing] environment entirely on me.”⁸

iv. Specifically, SCHULTE wrote that inadequate CIA security measures had “left [the CIA Group’s LAN] open and easy for anyone to gain access and easily download [from the LAN] and upload [sensitive CIA Group computer code] in its entirety to the [public] internet.”

b. It appears that SCHULTE did not, in fact, submit the Draft Resignation

⁸ SCHULTE went on to describe other complaints he had about managers at the CIA. Among other things, SCHULTE described his complaints about the way in which CIA Group management had handled various personnel and disciplinary issues (*see supra* at Part II.G.16).

Letter.

c. On his last day with the CIA (November 10, 2016), SCHULTE did, however, send an internal email to the CIA Office of the Inspector General (OIG) advising that office that he had been in contact with the United States House of Representatives' Permanent Select Committee on Intelligence regarding his complaints about the CIA ("OIG Email").

i. In the OIG Email, which SCHULTE labeled "Unclassified," SCHULTE raised many of the same complaints included in the draft "Letter of Resignation 10/12/16," described above, including the CIA's treatment of him and its failure to address the "security concerns" he had repeatedly raised in the past.

ii. Shortly thereafter, CIA security learned that one of SCHULTE's colleagues had witnessed SCHULTE printing the OIG Email, placing it in a folder, and exiting the CIA Component facility where SCHULTE worked.

iii. Notwithstanding SCHULTE's labeling of the email as "Unclassified," the CIA subsequently determined that the OIG Email which SCHULTE removed from the CIA without authorization did, in fact, contain classified information.

I. SCHULTE's Recent Inquiries About the Status of the Investigation

20. Based on my conversations with other law enforcement agents and others, and my review of documents, I understand that, since the March 7, 2017 publication of the Classified Information on WikiLeaks, SCHULTE has repeatedly initiated contact, via telephone and text messages, with multiple of his former CIA Group colleagues. Those colleagues have reported that contact to government and law enforcement officials.

a. In those communications with his former colleagues, SCHULTE has repeatedly asked about the status of the investigation into the disclosure of the Classified Information.

b. SCHULTE has requested more details on the information that was disclosed.

c. SCHULTE has inquired of his interlocutors' personal opinions regarding who, within the CIA Group, each believes is responsible for the disclosure of the Classified Information. SCHULTE has also asked what other former CIA Group colleagues are saying about the disclosure.

d. SCHULTE has repeatedly denied any involvement in the disclosure of the Classified Information.

e. SCHULTE has indicated the he believes that he is a suspect in the investigation of the leak of Classified Information.

f. I am not aware of any other former CIA employee who has initiated any contact with former colleagues regarding the disclosure of the Classified Information.

J. SCHULTE' s Planned Travel

21. Based on my conversations with other law enforcement agents and others, and my review of documents, including information provided by the Department of Homeland Security, I understand that SCHULTE has booked an international flight departing in four days—Thursday, March 16, 2017. (Return travel to the United States is booked for a few days later.) The aforementioned records and conversations reflect that this is only SCHULTE's second trip reflected in in DHS records outside the United States.

K. Probable Cause Justifying Search of the Subject Premises

22. Thus, based on the above, I submit that there is probable cause to believe that SCHULTE has committed by the Subject Offenses by stealing a substantial amount of classified information from the CIA and has transmitting that information to individuals not authorized to receive it, thereby endangering the nation's national security. Based on my training and

experience, I know that individuals who are involved in the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials use computers and other electronic devices in furtherance of their criminal activities. Based on my training and experience, I also know that individuals typically keep their computers and other electronic devices in their homes.

23. Based on my participation in this investigation, I believe that SCHULTE resides at the Subject Premises. Among other things, I have reviewed records provided by SCHULTE's employer in New York City, which indicate that SCHULTE resides at the Subject Premises. I have also reviewed SCHULTE's credit card records, which reflect that SCHULTE resides at the Subject Premises. I have also spoken with other law enforcement officers who have observed SCHULTE enter and exit the Building on several occasions since on or about March 8, 2017. Those law enforcement officers have also told me that the Building has an electronic directory that lists SCHULTE's name as the individual residing in the Subject Premises.

L. Probable Cause Justifying Search of ESI

24. As noted above, individuals who engage in the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials often use computers and other electronic devices to store documents and records relating to their illegal activity. Individuals engaged in these activities use electronic devices to, among other things, store copies of classified documents or materials; engage in email correspondence relating to their illegal activity; store contact information of co-conspirators, including telephone numbers, email addresses, and identifiers for instant messaging and social medial accounts; and/or store records of illegal transactions involving classified documents.

25. Individuals who engage in the criminal activity described herein, in the event that they change computers, will often back up or transfer files from their old computers' hard drives to that of their new computers, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity. In addition, individuals who engage in such criminal activity will often also store or transfer files on electronic storage media other than computer hard drives, including thumb drives, flash memory cards, CD-ROMs, or portable hard drives to, for example, facilitate the use of the information or to transfer it to co-conspirators in support of the criminal scheme.

26. Individuals who engage in criminal activity involving computers and electronic devices also often maintain physical evidence of their criminal activity, including, among other things, printouts of documents and records that are also stored electronically, as described above, or handwritten notes of the same, for example as a backup in case of a failure of the electronic media on which they were stored or to facilitate use of the data.

27. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files can be stored on a hard drive for years at little or no cost. Even when such files have been deleted, they can often be recovered, depending on how the hard drive has subsequently been used, months or years later with forensics tools. Specifically, when a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Deleted files, or remnants of deleted files, may accordingly reside in "slack space" (space that is not being used for storage of a file) for long periods of time before they are overwritten. In addition, a computer's operating system may keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via

the Internet are generally automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve from a hard drive or other electronic storage media depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits.

28. Based on the foregoing, I respectfully submit that there is probable cause to believe that SCHULTE is committing or has committed the Subject Offenses, and that evidence of this criminal activity is likely to be found in the Subject Premises and on computers and electronic media found in the Subject Premises.

III. Items to Be Seized

29. Closed or Locked Containers. Based on my training, experience, participation in this and other investigations, I know that individuals who participate in criminal activities routinely secrete and store books, records, documents, currency and other items of the sort described in Attachment A in secure locations like safety deposit boxes, suitcases, safes, key-lock strong boxes, and other types of locked or closed containers in an effort to prevent the discovery or theft of said items. The requested warrant and search procedure includes a search of any closed containers on the Subject Premises, including cabinets, vehicles, doors to rooms, sheds, outbuildings, and other appurtenances located on or within the Subject Premises whether they are locked or unlocked.

30. Electronic Devices. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the requested warrants would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. Based upon my training and experience and information related to me by agents and others involved in the forensic

examination of computers, I know that computer data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, thumb drives, magnetic tapes and memory chips. I also know that during the search of the Subject Premises it may not be possible to fully search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process, which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.

b. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the Subject Premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 160 gigabytes (GB) of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 80 million pages of data, which, if printed out, would result in a stack of paper over four miles high.

c. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files;

however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

31. In light of these concerns, I hereby request the Court’s permission to copy at the Subject Premises information stored on computer hardware (and associated peripherals) that may contain some or all of the evidence described in Attachment A hereto, and to conduct an off-site search of such copies for the evidence described, using the general procedures described in Attachment A. However, to the extent law enforcement is unable to copy electronic devices at the Subject Premises, I hereby request the Court’s permission to seize those devices and search them off-site.

IV. Procedures for Searching ESI

A. Execution of Warrant for ESI

32. Federal Rule of Criminal Procedure 41(e)(2)(B) provides that a warrant to search for and seize property “may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information . . . for later review.” Consistent with Rule 41, this application requests authorization to search and/or seize any computer devices and storage media and transport them to an appropriate law enforcement facility for review. This is typically necessary for a number of reasons:

- First, the volume of data on computer devices and storage media is often impractical for law enforcement personnel to review in its entirety at the search location.
- Second, because computer data is particularly vulnerable to inadvertent or intentional modification or destruction, computer devices are ideally examined in a controlled environment, such as a law enforcement laboratory, where trained personnel, using specialized software, can make a forensic copy of the storage media that can be subsequently reviewed in a manner that does not change the underlying data.
- Third, there are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized personnel and equipment potentially required to safely access the underlying computer data.
- Fourth, many factors can complicate and prolong recovery of data from a computer device, including the increasingly common use of passwords, encryption, or other features or configurations designed to protect or conceal data on the computer, which often take considerable time and resources for forensic personnel to detect and resolve.

B. Review of ESI

33. Following the search of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained therein for information responsive to the warrant.

34. In conducting this review, law enforcement personnel may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- conducting a file-by-file review by “opening” or reading the first few “pages” of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);
- “scanning” storage areas to discover and possibly recover recently deleted data or deliberately hidden files; and
- performing electronic keyword searches through all electronic storage areas to determine the existence and location of search terms related to the subject matter of the investigation. (Keyword searches alone are typically inadequate to detect all information subject to seizure. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.)

35. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement personnel may need to conduct a complete review of all the ESI from searched devices or storage media to evaluate its contents and to locate all data responsive to the warrant.

C. Return of ESI

36. If the Government seizes any electronic devices, later determines that the electronic devices are no longer necessary to retrieve and preserve the data, and the items are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return these items, upon request. Computer data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the

offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the Subject Offenses.

V. Execution of the Search Warrant: Necessity of Covert Search and Delayed Notification

37. I respectfully request that the search warrant permit law enforcement agents to execute the search at any time in the day or night. I also respectfully request that the search warrant permit law enforcement agents to execute the search warrant covertly without advance or contemporaneous notice of the execution of the warrant, or if they deem covert execution impracticable to execute the search warrant overtly without further order of the Court. Law enforcement agents will provide notice of the execution of the warrant, if it is executed covertly, within seven days of execution unless there is a new showing, made to the Court, that delayed notice is appropriate. If the warrant is executed overtly, notice will be provided at or as soon as practicable after the execution.

a. As described in greater detail above and below, there is probable cause to believe that SCHULTE has stolen a substantial amount of classified information and transmitted that information to those not authorized to receive it, thereby endangering the nation's national security.

b. SCHULTE likely engaged in these activities by using sophisticated computer skills to exfiltrate a substantial amount of data onto a removable drive and then covertly removed that drive from the CIA.

c. If SCHULTE is provided advance or contemporaneous notice of the execution of this search warrant, it may allow him to destroy evidence of his crimes on electronic devices by, for example, deleting drives or activating encryption programs that would make his devices virtually impossible to access.

d. Moreover, law enforcement agents will likely need some time to review and analyze any electronic devices identified at the Subject Premises. If SCHULTE is provided advance or contemporaneous notice of the search of the Subject Premises, he may be able to destroy evidence that can be developed based on the search of electronic devices.

38. Pursuant to Title 18, United States Code, Section 3103a(b)(1), delayed notification may be provided for a search warrant obtained pursuant to Rule 41 of the Federal Rules of Criminal Procedure if “the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result.” Delayed notification pursuant to this provision may only be provided for a reasonable period not to exceed 30 days, although it may be extended by the court for good cause shown, pursuant to Title 18, United States Code, Sections 3103a(b)(3) and 3103(c). A delayed notice warrant obtained pursuant to this provision prohibits “the seizure of tangible property, any wire electronic communication (as defined in section 2510), or, except as expressly provided in chapter 121, any stored wire or electronic information, *except where the court finds reasonable necessity for the seizure.*” Title 18, United States Code, Section 3103(b)(2) (emphasis added).

39. The investigation of the Subject Offenses and SCHULTE is on-going, and remains extremely sensitive. The FBI is continuing to review an enormous volume of electronic evidence, much of which remains highly classified and extremely sensitive. In addition, based on *inter alia* the statements in WikiLeaks March 7, 2017 press release accompanying the Classified Information, it appears at least possible that additional CIA information may have been stolen and provided to WikiLeaks or others not authorized to receive it. Accordingly, ensuring that the investigation remains covert for as long as possible is at its zenith. Public disclosure of the search prematurely could cause evidence to be destroyed or additional information to be hastily released


onto the Internet. In that context, I know, based on my review of the WikiLeaks press release, that they claimed to have refrained from publishing additional information they purport to possess such as “‘armed’ cyberweapons,” which I understand based on my training, experience and involvement in this investigation to mean the specific computer code they claim could actually be used to perpetrate a cyber-attack or penetration). They also claim to have “anonymi[zed] some identifying information,” which I understand, based on my training, experience, and involvement in this investigation, to include the names of covert CIA operatives and possibly covert United States Government locations. Finally, because SCHULTE has booked an overseas trip for this Thursday, it is critical that, to the extent possible, the search be conducted in such a way as to minimize the possibility that it causes him to flee or to destroy evidence. In light of the foregoing, it is reasonably necessary to conduct the search requested herein covertly.

40. Consistent with Title 18, United States Code, Section 3103a(b)(2), this application requests that any notice otherwise required for the seizure and search of information be delayed for a period of 30 days in light of the reasonable necessity – comprising both the investigatory aims and mitigating goals of this investigation – for such a delay.

VI. Conclusion and Ancillary Provisions

41. Based on the foregoing, I respectfully request the court to issue a warrant to search and seize the items and information specified in Attachment A to this Affidavit and to the Search and Seizure Warrant.

42. In light of the confidential nature of the continuing investigation, I respectfully request that this Affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise.



JEFF D. DONALDSON
Special Agent
Federal Bureau of Investigation

Sworn to before me on
this 13th day of March 2017


S/Barbara Moses

THE HONORABLE BARBARA MOSES
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK

Attachment A

I. Premises to be Searched—Subject Premises

The premises to be searched (the “Subject Premises”) is described as follows, and includes all locked and closed containers found therein:

The Subject Premises is particularly described as apartment 8C in a building located at 200 East 39th Street, New York, New York 10016 (the “Building”). The Building is located near the corner of 39th Street and Third Avenue. The Building is nineteen stories high and contains approximately ninety-one apartment units. The Subject Premises is a one-bedroom apartment located on the eighth floor of the Building, and it is clearly identifiable as apartment 8C from the outside of the Subject Premises.

II. Execution of the Warrant

Law enforcement agents are permitted to execute the search warrant at any time in the day or night, and further to execute the search warrant covertly without advance or contemporaneous notice of the execution of the search warrant. Law enforcement agents will provide notice of the execution of the warrant within seven days of execution unless there is a new showing, made to the Court, that delayed notice is appropriate.

III. Items to Be Searched and Seized

A. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be searched and/or seized from the Subject Premises include the following evidence, fruits, and instrumentalities of: (i) the unauthorized possession and, *inter alia*, the communication of national defense information to someone not entitled to receive it, in violation of Title 18, United States Code, Section 793(d); (ii) the unlawful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); (iii) exceeding authorized access to a computer in order to obtain national defense information with reason to believe that information could be used to the injury of the United States and the advantage of a foreign nation and willfully transmitting that information to a person not entitled to receive it, in violation of Title

18, United States Code, Section 1030(a)(1); and (iv) intentionally exceeding authorized access and thereby obtaining information from a department or agency of the United States, in violation of Title 18, United States Code, Section 1030(a)(2)(B) (collectively, the “Subject Offenses”):

1. Evidence concerning occupancy or ownership of the Subject Premises, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys.

2. Evidence concerning the identity or location of, and communications with, any co-conspirators.

3. Any and all notes, documents, records, correspondence, or materials, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, and handwritten notes), pertaining to the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials.

4. Electronic devices (including but not limited to computers, tablets, smartphones, and cellular telephones) and storage media used in furtherance of the Subject Offenses, containing evidence of the Subject Offenses, or containing evidence authorized for seizure in paragraphs 1, 2 and 3 above. The term “storage media” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

5. Electronic forensic evidence relating to the Subject Offenses, including for any electronic device or storage media whose search and/or seizure is authorized by this warrant as described above in paragraph 4 (hereinafter, “Computers”¹), including:

- a. evidence of the times the Computers were used in furtherance of the Subject Offenses;
- b. passwords, encryption keys, and other access devices that may be necessary to access the Computers;
- c. documentation and manuals that may be necessary to access the Computers or to conduct a forensic examination of the Computers;
- d. evidence of software that would allow others to control the Computers, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- e. evidence indicating how and when the Computers were accessed or used in furtherance of the Subject Offenses;
- f. evidence indicating the Computers’ user’s/users’ state of mind as it relates to the Subject Offenses;
- g. evidence of the attachment to the Computers of other storage devices or similar containers for electronic evidence in furtherance of the Subject Offenses;

¹ The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

- h. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Computers;
- i. records of or information about Internet Protocol addresses used by the Computers;
- j. records of or information about the Computers' Internet activity in furtherance of the Subject Offenses, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

6. If law enforcement personnel seize the computer(s) or other electronic device(s), the personnel will search the computer and/or device(s) within a reasonable amount of time, not to exceed 60 days from the date of execution of the warrant. If, after such a search has been conducted, it is determined that a computer or device contains any data listed in paragraphs 1 through 3, the Government will retain the computer or device. If it is determined that the computer(s) or device(s) are no longer necessary to retrieve and preserve the data, and the items are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(b), such materials and/or equipment will be returned within a reasonable time. In any event, such materials and/or equipment shall be returned no later than 60 days from the execution of this warrant, unless further application is made to the Court.

B. Search and Seizure of Electronically Stored Information

The items to be searched and seized from the Subject Premises also include any computer devices and storage media that may contain any electronically stored information falling within the categories set forth in Section III.A of this Attachment above, including, but not limited to,

desktop and laptop computers, disk drives, modems, thumb drives, personal digital assistants, smart phones, digital cameras, and scanners. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

The items to be searched and seized from the Subject Premises also include:

1. Any items or records needed to access the data stored on any seized or copied computer devices or storage media, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.
2. Any items or records that may facilitate a forensic examination of the computer devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.
3. Any evidence concerning the persons with access to, control over, or ownership of the seized or copied computer devices or storage media.

C. Review of ESI

Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques, including but not limited to:

- surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few "pages" of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files;
- scanning storage areas for deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- making reasonable efforts to utilize computer search methodology to search only for files, documents, or other electronically stored information within the categories identified in Sections I.A and I.B of this Attachment.

Exhibit C
Subject Devices Seized from Schulte Residence

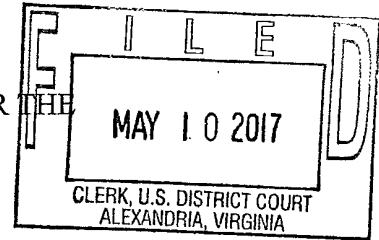
FBI Item #	Description
1B56	Rack server, no serial number
1B55	Black tower computer, no serial number
1B54	One bag containing seven CD/DVDs
1B53	One bag containing twenty-seven CD/DVDs
1B52	One bag containing twenty-eight CD/DVDs
1B51	One bag containing twenty-nine CD/DVDs
1B50	One bag containing fifteen CD/DVDs
1B49	One bag containing 9 floppy disks, and five CD/DVDs
1B48	One ATT Sim Card
1B47	One 16GB Micro SD
1B46	One 8 GB SanDisk Micro SD
1B45	One UFCU 128MB Thumb Drive
1B44	One Sans Thumb Drive
1B43	One SanDisk 1GB Thumb Drive
1B42	One PNY 1GB Thumb Drive
1B41	One OSR Thumb Drive
1B40	One SanDisk USB Thumbdrive 16GB
1B39	One TP-Link Network USB
1B38	One Garmin NUVI S/N: 1C2041768
1B37	One HTC Phone S/N: HT806G001901
1B36	One MS ZUHE Mp3 Player S/N: 014195164210
1B35	One Olympus Camera JOH244018
1B34	One HTC Cell Phone S/N: HTO68P900155
1B33	One Samsung Phone Model: SPHL710
1B32	One Western Digital 1 TB Hard Disk Drive ("HDD") S/N: WCAW32653861
1B31	One 640 GB Western Digital HDD S/N: WCASY0416918
1B30	One 160GB Western Digital HDD S/N: WMAU2U189169
1B29	One Samsung 1 TB HDD S/N: 52AEJ18Z408962
1B28	One Samsung 1 TB HDD S/N: S2AEJ18Z4408961
1B27	One Samsung 1 TB HDD S/N: S2AEJ18Z408963
1B26	One Western Digital 1 TB Hard Drive ("HD") S/N: WCAU45276871
1B25	One Western Digital 1 TB HDD S/N: WCAU42139599
1B24	One Western Digital 1 TB HDD S/N: WCAW32328401
1B23	One Western Digital 1 TB HDD S/N: WCAU45355046
1B22	One Kingston Hyper X Solid State Drive ("SSD")
1B21	One 120GB Samsung SSD S19HNSAD5517655
1B20	One black server tower, no serial number
1B19	One Samsung Phone Model SM-J320P
1B18	One Kindle
1B17	One Samsung tablet S/N: R52H60LF5RY
1B16	One Kindle
1B15	One Xbox1 S/N: 149212254048
1B14	One Xbox 360s S/N: 033320322443

Exhibit C
Subject Devices Seized from Schulte Residence

FBI Item #	Description
1B13	One SanDisk MP3 Player
1B12	One SanDisk MP3 Player
1B10	One SanDisk Thumbdrive
1B9	One black server tower

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN THE MATTER OF THE SEARCH OF:) **UNDER SEAL**
Electronic Devices Previously Seized from the)
Premises of 200 East 39th Street, Apartment 8C,) Case No. 1:17-SW-243
New York, NY 10016)

**GOVERNMENT'S MOTION TO SEAL SEARCH WARRANT
PURSUANT TO LOCAL RULE 49(B)**

The United States of America, by and through undersigned counsel, upon the return of its executed search warrant,¹ and pursuant to Local Rule 49(B) of the Local Criminal Rules for the United States District Court for the Eastern District of Virginia, now asks for an Order to Seal the search warrant, application for the search warrant and the affidavit in support of the search warrant, together with this Motion to Seal and proposed Order, until the United States makes a motion to unseal the search warrant and affidavit.

I. REASONS FOR SEALING (See Local Rule 49(B)(1))

1. At the present time, Special Agents of the Federal Bureau of Investigation (FBI) are conducting an investigation into: (i) violations of Title 18, United States Code, Section 2252 (possession, transportation, receipt, distribution, production, and reproduction of sexually explicit material relating to children) and Title 18, United States Code, Section 2252A (activities relating to material constituting or containing child pornography); and (ii) violations of Title 17, United States Code, Section 506 and Title 18, United States Code, Section 2319 (criminal infringement of a copyright).

¹ Pursuant to Local Rule 49(B), "[n]o separate motion to seal is necessary to seal a search warrant *from the time of issuance to the time the executed warrant is returned.*" (Emphasis added.) This is because, as Rule 49(B) additionally mandates, "[u]ntil an executed search warrant is returned, search warrants and related papers are not filed with the Clerk."

2. Premature disclosure of the specific details of this ongoing investigation (as reflected, for example, in the affidavit in support of search warrant) would jeopardize this continuing criminal investigation and may lead to the destruction of additional evidence in other locations. Thus, a sealing order is necessary to avoid hindering the ongoing investigation in this matter.

3. The United States has considered alternatives less drastic than sealing, including, for example, the possibility of redactions, and has determined that none would suffice to protect this investigation.

II. THE GOVERNING LAW (See Local Rule 49(B)(2))

4. It is generally recognized that the public has a common law right of access, but not a First Amendment right of access, to judicial documents, including documents associated with *ex parte* proceedings such as search warrant affidavits. Media General Operations, Inc. v. Buchanan, 417 F.3d 424, 429 (4th Cir. 2005); In re Washington Post Company v. Hughes, 923 F.2d 324, 326 (4th Cir. 1991). “But the right of access is qualified, and a judicial officer may deny access to search warrant documents if sealing is ‘essential to preserve higher values’ and ‘narrowly tailored to serve that interest.’” Media General Operations, 417 F.3d at 429 (citations omitted); see also In re Knight Pub. Co., 743 F.2d 231, 235 (4th Cir. 1984) (“[t]he trial court has supervisory power over its own records and may, in its discretion, seal documents if the public’s right of access is outweighed by competing interests”). Sealing search warrants and their accompanying affidavits and application is within the discretionary powers of a judicial officer where, among other things, an “‘affidavit contain[s] sensitive details of an ongoing investigation’ and it is ‘clear and apparent from the affidavits that any disclosure of the

information there would hamper' th[e] ongoing investigation." Media General Operations, 417 F.3d at 430 (citations omitted); see also In re Search Warrant for Matter of Eye Care Physicians of America, 100 F.3d 514, 518 (7th Cir. 1996).

5. Before a district court generally may seal judicial records or documents, it must (a) provide public notice of the request to seal and allow interested parties a reasonable opportunity to object, (b) consider less drastic alternatives to sealing the documents, and (c) provide specific reasons and factual findings supporting its decision to seal the documents and for rejecting the alternatives. Ashcraft v. Conoco, Inc., 218 F.3d 288, 302 (4th Cir. 2000).

6. However, regarding the notice requirement in the specific context of a search warrant, the Fourth Circuit has cautioned that "the opportunity to object" cannot "arise prior to the entry of a sealing order when a search warrant has not been executed." Media General Operations, 417 F.3d at 429. "A rule to the contrary would endanger the lives of officers and agents and allow the subjects of the investigation to destroy or remove evidence before the execution of the search warrant." Id.; see also Franks v. Delaware, 438 U.S. 154, 169 (1978). Accordingly, in the context of search warrants, "the notice requirement is fulfilled by docketing 'the order sealing the documents,' which gives interested parties the opportunity to object after the execution of the search warrants." Media General Operations, 417 F.3d at 430 (quoting Baltimore Sun Co. v. Goetz, 886 F.2d 60, 65 (4th Cir. 1989)); see also Local Rule 49(B) ("Until an executed search warrant is returned, search warrants and related papers are not filed with the Clerk.").

7. As to the requirement of a court's consideration of alternatives, the Fourth Circuit counsels that, "[i]f a judicial officer determines that full public access is not appropriate, she 'must consider alternatives to sealing the documents,' which may include giving the public

access to some of the documents or releasing a redacted version of the documents that are the subject to the government's motion to seal.” Media General Operations, 417 F.3d at 429 (quoting Goetz, 886 F.2d at 66).

8. Finally, regarding the requirement of specific findings, the Fourth Circuit's precedents state that, “in entering a sealing order, a ‘judicial officer may explicitly adopt the facts that the government presents to justify sealing when the evidence appears creditable,’” Media General Operations, 417 F.3d at 429 (quoting Goetz, 886 F.2d at 65), so long as the ultimate “decision to seal the papers” is “made by the judicial officer,” Goetz, 886 F.2d at 65. “Moreover, if appropriate, the government’s submission and the [judicial] officer’s reason for sealing the documents can be filed under seal.” Goetz, 886 F.2d at 65; see also In re Washington Post Co., 807 F.2d 383, 391 (4th Cir. 1986) (“if the court concludes that a denial of public access is warranted, the court may file its statement of the reasons for its decision under seal”).

III. PERIOD OF TIME GOVERNMENT SEEKS TO HAVE MATTER REMAIN UNDER SEAL (See Local Rule 49(B)(3))

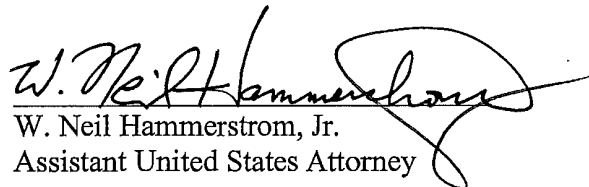
9. Pursuant to Local Rule 49(B)(3), the search warrant and the affidavit will remain sealed until the need to maintain the confidentiality of the search warrant application and the related investigation expires, after which time the United States will move to unseal the search warrant and affidavit.

WHEREFORE, the United States respectfully requests that the search warrant, application for search warrant, affidavit in support of the search warrant, and this Motion to Seal and proposed Order be sealed until further Order of the Court.

Respectfully submitted,

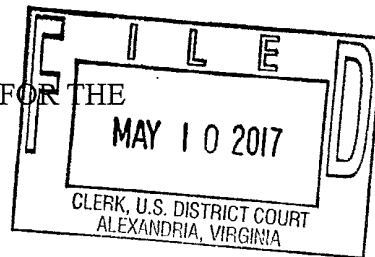
Dana J. Boente
United States Attorney

By:


W. Neil Hammerstrom, Jr.
Assistant United States Attorney

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN THE MATTER OF THE SEARCH OF:)
Electronic Devices Previously Seized from the)
Premises of 200 East 39th Street, Apartment 8C,)
New York, NY 10016)

UNDER SEAL

Case No. 1:17-SW-243

ORDER TO SEAL

The UNITED STATES, pursuant to Local Rule 49(B) of the Local Criminal Rules for the United States District Court for the Eastern District of Virginia, having moved to seal the search warrant, the application for search warrant, the affidavit in support of the search warrant, the Motion to Seal, and proposed Order in this matter; and

The COURT, having considered the government's submissions, including the facts presented by the government to justify sealing; having found that revealing the material sought to be sealed would jeopardize an ongoing criminal investigation; having considered the available alternatives that are less drastic than sealing, and finding none would suffice to protect the government's legitimate interest in concluding the investigation; and having found that this legitimate government interest outweighs at this time any interest in the disclosure of the material; it is hereby

ORDERED, ADJUDGED, and DECREED that, the search warrant, application for search warrant, affidavit in support of the search warrant, Motion to Seal, and this Order be sealed until further Order of the Court.

_____/s/_____
Michael S. Nachmanoff
United States Magistrate Judge
Michael S. Nachmanoff
United States Magistrate Judge

Date: 5/10/17
Alexandria, Virginia

UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

Electronic Devices Previously Seized from the
Premises of 200 East 39th Street, Apartment 8C,
New York, NY 10016

Case No. 1:17-SW-243

UNDER SEAL

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Eastern District of Virginia
(identify the person or describe the property to be searched and give its location):

Electronic devices located at a U.S. Government facility in Herndon, Virginia

The person or property to be searched, described above, is believed to conceal (identify the person or describe the
property to be seized):

SEE ATTACHMENT A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or
property.

YOU ARE COMMANDED to execute this warrant on or before May 24, 2017

(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m. ☒ at any time in the day or night as I find reasonable cause has been
established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property
taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the
place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an
inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge
Michael S. Nachmanoff

(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay
of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be
searched or seized (check the appropriate box) ☐ for _____ days (not to exceed 30).

☐ until, the facts justifying, the later specific date of _____Date and time issued: 5/10/17 @ 12:00 p

Michael S. Nachmanoff MA
United States Magistrate Judge
Judge's signature

City and state: Alexandria, Virginia
Michael S. Nachmanoff, United States Magistrate Judge
Printed name and title

BY

DEPUTY CLERK

AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

Return

Case No.: 1:17-SW-_____	Date and time warrant executed:	Copy of warrant and inventory left with:
----------------------------	---------------------------------	--

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

Attachment A

I. Devices to be Searched—Subject Devices

The devices to be searched (the “Subject Devices”) include any and all electronic devices seized pursuant to a search warrant executed on or about March 15, 2017 at the premises described as apartment 8C in a building located at 200 East 39th Street, New York, New York 10016.

II. The Search of the Subject Devices

A. Evidence, Fruits, and Instrumentalities of the Child Pornography Offenses

The Subject Devices may be searched for the following evidence, fruits, and/or instrumentalities of violations of Title 18, United States Code, Sections 2252 (activities relating to material constituting or containing child pornography) and 2252A (possession, transportation, receipt, distribution, production, and reproduction of sexually explicit material relating to children) (the “CP Offenses”):

- Evidence of computer programs used to access, transmit, or store information relating to the CP Offenses;
- Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from computer devices, storage media, and related electronic equipment;
- Evidence of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
- Motion pictures, films, videos, and other recordings of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
- Correspondence and records pertaining to violation of the CP Offenses including, but not limited to electronic mail, chat logs, electronic messages, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions involving any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
- Records or other items which evidence ownership, control, or use of, or access to computer devices, storage media, and related electronic equipment used to access, transmit, or store information relating to the CP Offenses, including but not limited to sales receipts, warranties, bills for internet access, registry entries, configuration files, saved usernames and passwords, user profiles, email contacts, and photographs.

- Information or correspondence pertaining to affiliation with any child exploitation bulletin boards, chat forums, or organizations;
- Any child pornography as defined by 18 U.S.C. § 2256(8);
- Any child erotica, defined as suggestive visual depictions of nude minors which do not constitute child pornography as defined by 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined by 18 U.S.C. § 2256(2);
- Notes, documents, records, invoices, or correspondence, in any format and medium, including, but not limited to, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);
- Names, and lists of names and addresses of individuals (including minors) related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);
- Mailing lists and/or supplier lists related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2); and
- Financial records, including credit card information, bills, and payment records related to related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

B. Evidence, Fruits, and Instrumentalities of the Copyright Offenses

The Subject Devices may also be searched for the following evidence, fruits, and/or instrumentalities of violations of violations of 17 U.S.C. § 506 and 18 U.S.C. § 2319 (criminal infringement of a copyright) (the “Copyright Offenses”):

- Evidence of computer programs used to transmit or store information relating to the Copyright Offenses;
- Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from computer devices, storage media, and related electronic equipment;

- Evidence of copyrighted works, including motion pictures, films, videos, other recordings, and documents relating to the Copyright Offenses;
- Correspondence and records pertaining to violation of the Copyright Offenses including, but not limited to electronic mail, chat logs, electronic messages, and records bearing on the transmission, receipt, and/or storage of copyrighted works;
- Records or other items which evidence ownership, control, or use of, or access to computer devices, storage media, and related electronic equipment used to transmit or store information relating to the Copyright Offenses, including but not limited to sales receipts, warranties, bills for internet access, registry entries, configuration files, saved usernames and passwords, user profiles, email contacts, and photographs.
- Any copyrighted works;
- Notes, documents, records, invoices, or correspondence, in any format and medium, including, but not limited to, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, related to the transmission, receipt, and/or storage of copyrighted works;
- Names, and lists of names and addresses of individuals (including minors) related to the transmission, receipt, and/or storage of copyrighted works;
- Mailing lists and/or supplier lists related to the transmission, receipt, and/or storage of copyrighted works; and
- Financial records, including credit card information, bills, and payment records related to the transmission, receipt, and/or storage of copyrighted works.

C. Review of ESI

In conducting a review of ESI on the Subject Devices, law enforcement personnel may use various techniques, including but not limited to:

- surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files;
- scanning storage areas for deliberately hidden files;

- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- making reasonable efforts to utilize computer search methodology to search only for files, documents, or other electronically stored information within the categories identified in Section II.A of this Attachment.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Section II.A and II.B. of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all ESI from the Subject Devices if necessary to evaluate its contents and to locate all data responsive to the warrant.

17 MAG 3734

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All Content and
Other Information for the Google account
associated with Email Address
joshschulte1@gmail.com, Maintained at
Premises Controlled by Google, Inc. and Google
Payment Corp.

TO BE FILED UNDER SEAL

Agent Affidavit in Support of
Application for Search Warrant

**Application for a Search Warrant
for Stored Electronic Communications**

STATE OF NEW YORK)
) ss.
COUNTY OF NEW YORK)

JEFF D. DONALDSON, being duly sworn, deposes and says:

I. Introduction

A. Affiant

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI") assigned to the New York Field Office, and have been employed by the FBI since 2010. I am currently assigned to a squad responsible for counterespionage matters and have worked in the field of counterintelligence from 2010 to present. In the course of my duties as a Special Agent, I am responsible for investigating offenses involving espionage and related violations of law, including unauthorized retention, gathering, transmitting or losing classified documents or materials; unauthorized removal and retention of classified documents or materials; illegally acting in the United States as a foreign agent; other national security offenses; and the making of false statements. As a result of my involvement in espionage investigations and investigations involving the unauthorized disclosure or retention of classified information, as well as my training in counterintelligence operations, I am familiar with the tactics, methods, and techniques of United States persons who possess, or have possessed a United States Government security clearance and

may choose to harm the United States by misusing their access to classified information. I am also familiar, though my training and experience with the use of computers in criminal activity and the forensic analysis of electronically stored information.

2. **Basis for Knowledge.** This Affidavit is based upon my participation in the investigation, my examination of reports and records, and my conversations with other law enforcement agents and other individuals, as well as my training and experience. Because this Affidavit is being submitted for the limited purpose of obtaining the Requested Information, it does not include all the facts that I have learned during the course of this investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated. In addition, unless otherwise indicated, statements by others referenced in this Affidavit were not necessarily made to me, but may have been provided to me by someone else to whom I have spoken or whose report I have read (and who in turn may have had either direct or indirect knowledge of the statement). Similarly, unless otherwise indicated, information in this Affidavit resulting from surveillance does not necessarily set forth my personal observations, but may have been provided to me by other law enforcement agents who observed the events, and to whom I have spoken or whose report I have read.

II. The Target Account

3. I make this Affidavit in support of an application for a search warrant pursuant to 18 U.S.C. § 2703 directed to Google, Inc. and Google Payment Corp. (collectively “Google” or the “Provider”), headquartered in Mountain View, CA, for all content and other information associated with the following “**Target Account**”: the Google account associated with the email address joshschulte1@gmail.com, which is maintained and controlled by Google.

4. On or about March 14, 2017, the Honorable Barbara C. Moses issued a search warrant for all content and other information associated with the **Target Account** (the “March 14 Target Account Search Warrant”), which was issued in connection with an investigation into the unlawful retention and dissemination of classified materials. Following the execution of the March 14 Target Account Search Warrant, the investigation has revealed that the **Target Account** is likely to contain evidence, fruits, and instrumentalities of offenses involving child pornography and copyright infringement, in addition to offenses relating to the retention and dissemination of classified materials.

5. Based on returns obtained pursuant to the March 14 Target Account Search Warrant, as well as other evidence encountered in this investigation as described below, this application seeks a search warrant (a) directing Google to provide all content and information associated with the **Target Account**; (b) authorizing the review of content and other information associated with **Target Account** for evidence, fruits, and instrumentalities of the offenses relating to the unlawful retention and dissemination of classified materials (described further below and in Attachment A) from March 14, 2017 to the present; and (c) authorizing the search of content and other information associated with of the **Target Account** for evidence, fruits, and instrumentalities of offenses relating to child pornography and copyright infringement (described further below and in Attachment A) from May 17, 2007 through the present.

6. Based on my training, experience, and participation in this investigation, I know the following about Google:

a. Google offers email and other Internet-based services to the public. Among other things, Google allows subscribers to maintain email accounts under the domain name gmail.com. A subscriber using Google’s services can access his or her email account from any

computer connected to the Internet, and can link any variety of Google's other Internet-based services to his/her Gmail account.

b. Google maintains the following records and information with respect to every subscriber account:

i. *Email contents.* In general, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account, is maintained on Google's servers unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on Google's computers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

ii. *Address book.* Google also allows subscribers to maintain the equivalent of an address book, comprising email addresses and other contact information of other email users.

iii. *Subscriber and billing information.* Google collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. Google also maintains records concerning the date on which the account was created, the Internet protocol ("IP") address of the user at the time of account creation, the current status of the account (*e.g.*, active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying subscribers, Google maintains records of the subscriber's means and source of payment, including any credit card or bank account number.

iv. *Transactional information.* Google also typically retains certain transactional information about the use of each account on its system. This information can include

records of login (*i.e.*, session) times and durations and the methods used to connect to the account (such as logging into the account through Google's website).

v. *Linked Accounts.* Google also typically maintains records of other Google accounts likely sharing a common owner with a target account. Google may identify such accounts through the use of "cookie" files that reveal when the same web browser is used to log in to multiple Google accounts, or by comparing subscriber information across its records to identify accounts that share, *e.g.*, a recovery email account or phone number.

vi. *Customer correspondence.* Google also typically maintains records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber's account.

vii. *Preserved records.* Google also maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f).

c. In addition, subscriber information for the **Target Account** indicates that the subscriber of the **Target Account** has activated additional online Google Services, and, accordingly, the Provider also maintains, among other things, the following records and information with respect to the **Target Account**:

i. *Google Drive.* Google provides users with a certain amount of free "cloud" storage, currently 15 gigabytes, through the service called "Google Drive" (users can purchase a storage plan through Google to store additional content). Users can use their Google Drive to store email, attachments, videos, photographs, documents, and other content "in the cloud," that is online. A user can access content stored on Google Drive by logging into his or her Google account through any computer or other electronic device that is connected to the Internet.

Users can also share files stored on Google Drive with others, allowing them to view, comment, and/or edit the files

ii. *Google Docs.* Google provides users with the ability to write, edit, and collaborate on various documents with other Google users through a service called “Google Docs.” Users can use Google Docs to create online documents that can be stored on or saved to the user’s Google Drive. Users can also download such documents in various formats, such as a Microsoft Word document (e.g., “.docx”), an OpenDocument Format (“.odt”), Rich Text Format (“.rtf”), a PDF document (“.pdf”), or Plain Text document (“.txt”).

iii. *Google Photos.* Google provides users with a certain amount of free storage for photographs, through a service called Google Photos, which allows users to manually store photographs and videos, and which automatically uploads photographs and videos taken by registered mobile devices. Google also retains the metadata—or data that provides information about the data in question, such as the time and date of creation, the author or creator, the means of its creation, the purpose of the data, among other data—for photos and videos that are uploaded to Google, including to Google Photos. This metadata includes what is known as exchangeable image file format (or “Exif”) data, and can include GPS location information for where a photo or video was taken.

iv. *Google Calendar.* Google provides users with an online calendar, in which they can add appointments, events, and reminders, which are synchronized across registered computers and mobile devices. Users can share their calendars with other users, allowing the maintenance of joint calendars.

v. *YouTube content.* Google allows subscribers to maintain linked YouTube accounts, a global video-sharing website that allows users to upload and share videos

with public on the Internet. Registered users can upload an unlimited number of videos and add comments to videos.

vi. *Google Chats and Google Hangouts content.* Google allows subscribers to engage in “chat” sessions in an instant messaging format with other Google users, the transcripts of which are generally stored in a user’s email content. Similarly, Google allows users to engage in enhanced chat sessions, called Hangouts, which permit the sharing of additional content such as videos, sounds, and images. In general, Hangouts content is stored separately from a user’s email and chat content.

vii. *Location history data.* Google maintains recent location data, collected periodically, from mobile devices that are logged into or have used applications (or “apps”) or services provided by Google. For example, Google collects information collected from GPS, Wi-Fi networks, cell site locations, and mobile networks to estimate a user’s location. Google apps and services also allow for location reporting, which allows Google to periodically store and use a device’s most recent location data in connection with a Google account.

viii. *Android Services.* Google also maintains information relating to Android, as it relates to an account. Android is a mobile operating system that is developed by Google, and is used on a variety of touchscreen mobile devices, such as smartphones and tablet computers. Google retains information related to the Android device associated with an account, including the IMEI (the International Mobile Station Equipment Identifier), MEID (the Mobile Equipment Identifier), device ID, Google-assigned Advertising ID, and/or serial number of the devices. Each of those identifiers uniquely identifies the device used. One device may be associated with multiple different Google and Android accounts, and one Google or Android account may be associated with multiple devices.

ix. *Google Voice.* Google provides a telephone service that provides call forwarding and voicemail services, voice and text messaging.

x. *Google Payments and Wallet.* Google allows for the storage of payment information associated with a Google Account, including credit cards and bank accounts, and contains information about all transactions made with a Google account, allowing for the payment for goods (such as those purchased through Google Shopping) and bills, and the transfer of money by subscribers using their Google Gmail address or phone number, among other features.

xi. *Web History.* Google maintains searches and account browsing activity, from Chrome, Google's proprietary web browser, as well as other Google applications. Some of this data is obtained through Google's advertising business, also known as DoubleClick.

III. Jurisdiction to Issue Requested Warrant

7. Pursuant to Title 18, United States Code, Sections 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as Google, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

8. A search warrant under Section 2703 may be issued by "any district court of the United States (including a magistrate judge of such a court)" that "has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

9. When the Government obtains records under Section 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A) & (3). Additionally, the Government may obtain an order precluding the Provider from notifying the subscriber or any other person of the warrant, for such period as

the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

IV. The Subject Offenses

10. For the reasons detailed below, I believe that there is probable cause that the **Target Account** contains evidence, fruits, and instrumentalities of (i) the unauthorized possession and, *inter alia*, the communication of national defense information to someone not entitled to receive it, in violation of Title 18, United States Code, Section 793(d); the unlawful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); exceeding authorized access to a computer in order to obtain national defense information with reason to believe that information could be used to the injury of the United States and the advantage of a foreign nation and willfully transmitting that information to a person not entitled to receive it, in violation of Title 18, United States Code, Section 1030(a)(1); and intentionally exceeding authorized access to a computer and thereby obtaining information from a department or agency of the United States, in violation of Title 18, United States Code, Section 1030(a)(2)(B) (the “National Security and Computer Crime Offenses”); (ii) violations of Title 18, United States Code, Section 2252 (possession, transportation, receipt, distribution, production, and reproduction of sexually explicit material relating to children) and Title 18, United States Code, Section 2252A (activities relating to material constituting or containing child pornography) (the “CP Offenses”); and (iii) violations of Title 17, United States Code, Section 506 and Title 18, United States Code, Section 2319 (criminal infringement of a copyright) (the “Copyright Offenses”) (collectively, with the National Security and Computer Crime Offenses and the CP Offenses, the “Subject Offenses”).

A. Terminology

11. The term “computer,” as used herein, is defined as set forth in 18 U.S.C. § 1030(e)(1).

12. The term child pornography is defined in Title 18, United States Code, Section 2256(8) in pertinent part as “any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where . . . the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct.”¹

13. The terms “Minor,” “Sexually Explicit Conduct” and “Visual Depiction” are defined as set forth in Title 18, United States Code, Section 2256.

V. Probable Cause and Request to Search

A. Probable Cause Relating to the National Security and Computer Crime Offenses

14. Based on my review of publicly available material on the Internet, including on the website wikileaks.org (“WikiLeaks”), I know that, on March 7, 2017, WikiLeaks published what it claimed were more than 8,000 documents and files that contained classified information (the “Classified Information”) belonging to the Central Intelligence Agency (“CIA”). In its press release accompanying the Classified Information, WikiLeaks further claimed that:

a. The public dissemination of the Classified Information was “the largest ever” unauthorized publication of classified CIA documents.

b. The Classified Information constituted the “first full part” of a series—thus indicating that there would be subsequent publications of additional sensitive CIA information.²

c. The “collection” obtained by WikiLeaks amounted to “more than several

¹ See also *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002) (analyzing constitutional validity of the definitions set forth in 18 U.S.C. § 2256(8)).

² On or about March 24, 2017, March 31, 2017, April 7, 2017, April 14, 2017, April 21, 2017, April 28, May 5, 2017, and May 12, 2017 WikiLeaks released additional batches of documents that it claimed were also obtained from the CIA.

hundred million lines of code” and revealed the “entire hacking capacity” of the CIA, including various malware, viruses, and other tools used by the CIA.

15. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that:

a. The information that WikiLeaks claimed was classified CIA information—that is, the Classified Information—was at the time of its disclosure, in fact, classified CIA information.

b. Specifically, the Classified Information was created and maintained by one specific group within the CIA which is responsible for various computer engineering activities, including the development of computer code (the “CIA Group”). That CIA Group exists within a larger CIA component (the “CIA Component”). In March 2016, less than 200 employees were assigned to the CIA Group.

c. The Classified Information was maintained by the CIA Group on an isolated local-area computer network (the “LAN”).³ Only employees of the CIA Group had access to the LAN on which the Classified Information was stored.⁴

³ In its press release announcing the publication of the Classified Information, WikiLeaks stated that the Classified Information originated from “an isolated, high-security network.”

⁴ Prior search warrant applications in connection with this investigation set forth that a preliminary analysis had concluded that the Classified Information was likely copied from a back-up server to which the same three systems administrators likely had access. The information that the Classified Information was likely recovered from an automated back-up file to which only systems administrators likely had access was first received by the FBI on or about March 22, 2017. As set forth herein, an investigation is ongoing as to whether the stolen data was in fact back-up data taken from the automated back-up. But, nevertheless, the current assessment remains that the copying of the data, regardless of the data’s original location, would likely have required systems administrator access of the type maintained by TARGET SUBJECT JOSHUA ADAM SCHULTE. Accordingly, I respectfully submit that the precise location from where the Classified Information was taken—whether from an automated back-up file or from a non-back-up computer file—does not affect the probable cause underlying the prior search warrant applications.

i. An isolated network, such as the CIA Group's LAN, is a network-security structure by which the isolated network is physically separated (or "air-gapped") from unsecured networks, such as the public Internet.

ii. Accordingly, such isolated networks, like the LAN, cannot be accessed from the public Internet, but rather only through those computers which are physically connected to the isolated network.

iii. The CIA Group's LAN, and each of its component parts, was maintained in heavily secured governmental facilities, which include multiple access controls and various other electronic and physical security measures.

d. Based on a preliminary analysis of the timestamps associated with the latest (or most recent) creation or modification date associated with the Classified Information, it appears that the Classified Information was copied from the LAN in or about March 2016.

e. The duplication and removal from the LAN of the Classified Information and its subsequent public dissemination via WikiLeaks was not authorized by the United States government.

f. The unauthorized disclosure of the Classified Information could—at a minimum—reasonably be expected to cause serious damage to the national security of the United States. *See* Executive Order 13526; 18 C.F.R. § 3a.11(a)(2).

g. The Classified Information is national defense information and its disclosure could reasonably be expected to be used to the injury of the United States and to the advantage of a foreign nation. *See* 18 U.S.C. § 793(d) & (e).

16. I know, based on my conversations with other law enforcement agents and others, that TARGET SUBJECT JOSHUA ADAM SCHULTE was employed as a computer engineer by

the CIA—specifically in the CIA Group—from in or about May 2010 through on or about November 10, 2016, when he resigned from the CIA. Based on those conversations, I understand the following about the nature of SCHULTE’s employment with the CIA, in substance and in part:

a. During SCHULTE’s more than six years working in the CIA Group, his responsibilities included, among other things, developing computer code for specific projects, including projects explicitly described in the Classified Information. SCHULTE had a skill set that enabled him to write computer code designed to clandestinely copy data from computers.

b. As part of his responsibilities with the CIA Group, in or about March and early April 2016, SCHULTE was one of three system administrators for the LAN. Among other things, that meant that he was one of three employees responsible for maintaining the LAN, and for controlling the access of other CIA Group employees.

c. These three systems administrators also had “super-user” access to the LAN, which allowed them broader access to programs, files and servers.

17. Based on my conversations with law enforcement officers and others, including individuals with an expertise in computer systems, and knowledge of the LAN, and my conversations with individuals who have conducted preliminary forensic analyses of the LAN and its related computer systems, I understand the following, in substance and in part:

a. Preliminary analysis suggests that the wholesale access to, and subsequent copying of, the Classified Information would likely have required systems administrator access of the type described above.⁵

⁵ I describe this as a “preliminary analysis” because analysis of the precise origin of the Classified Information is ongoing, and therefore the conclusions drawn from the preliminary analyses to date may be subject to modification once the analysis has been concluded. For example, among the facts that the FBI and CIA continue to analyze and verify is the precise number of individuals with “super-user” access who would have had access to the Classified Information during the relevant

b. The publicly released Classified Information originally published by WikiLeaks, based on a preliminary review, appears to contain the names and/or pseudonyms of, *inter alia*, multiple CIA employees—including two of the three aforementioned LAN systems administrators. SCHULTE's name, on the other hand, apparently was not published in the Classified Information. Thus, SCHULTE was the only one of the three systems administrators who was not publicly identified via WikiLeaks's first publication of the Classified Information.

c. The other two individuals who served in March 2016 as systems administrators for the CIA Group's LAN remain employed by the CIA. SCHULTE resigned from the CIA in November 2016, as described in detail below.

18. Based on my conversations with other law enforcement agents and others, my review of documents prepared by such law enforcement agents or obtained from the CIA, I know that SCHULTE has alleged that, on or about March 1, 2016, another CIA Group co-worker had made a threat against him. Based on those conversations and that review of documents regarding SCHULTE's threat allegations against his former co-worker, I understand the following, in substance and in part:

a. The CIA conducted an investigation into the incident, at the conclusion of

time period, which in and of itself is in part dependent upon the mechanism or route by which the Classified Information was obtained. Information the FBI received on April 5, 2017 revealed that there is a possibility that this number could have been slightly lower or slightly higher than the initial estimates set forth in prior search warrant affidavits submitted in the course of this investigation, and that such variation depends on the route through which the Classified Information was accessed. While there may have been multiple mechanisms to gain access to the Classified Information, the preliminary assessment is that the most likely routes to acquiring that information would have required systems administrator access. Notwithstanding that fact, it is, of course, also possible that an employee who was not a designated systems administrator could find a way to gain access to the Classified Information (*e.g.*, an employee could steal and use—without legitimate authorization—the username and password of a designated systems administrator, or an employee lacking systems administrator access could, at least theoretically, gain access to the Classified Information by finding a “back-door” to it).

which SCHULTE expressed deep unhappiness about the way that CIA responded to the alleged threat.

b. SCHULTE threatened legal action against the CIA for its handling of the situation, and repeatedly stated that he felt that he was being punished by CIA management for reporting the alleged threat incident.

c. SCHULTE informed CIA security that, if “forced into a corner” he would proceed with a lawsuit against the CIA. He also repeatedly threatened that he or his lawyer would go to the media.

d. In addition, CIA security learned that SCHULTE had removed an internal CIA document from CIA facilities that related to his complaints to the CIA concerning its handling of the alleged threat, despite being told multiple times by CIA security officials not to do so. On or about April 4, 2016, SCHULTE and the other CIA employee were reassigned to different offices within the CIA Group in response to SCHULTE’s allegations.

e. Around the time of his reassignment to another branch within the CIA Group, and at least in part because of his new responsibilities, many of SCHULTE’s administrator privileges on the LAN were revoked, and he was no longer permitted to serve as a systems administrator in the CIA Group’s LAN.

f. At approximately the same time, *i.e.*, on or about April 4, 2016, SCHULTE’s computer access to a specific developmental project (“Project-1”) was also revoked. Until his reassignment, SCHULTE had been the CIA Group employee with principal responsibility for Project-1. Upon SCHULTE’s transfer, principal responsibility for Project-1 was

transferred to another CIA Group employee, who received computer access to Project-1.⁶

19. I know from my review of publicly available material on the Internet, including WikiLeaks.org, that Project-1 was one of a small group of CIA projects and capabilities that WikiLeaks highlighted explicitly by name in its March 7, 2017 press release that accompanied the online publication of the Classified Information.

20. Based on my involvement in this investigation and my conversations with other FBI agents involved in this investigation, I know that on or about March 14, 2017, pursuant to the March 14 Target Account Search Warrant described above in paragraph 4, Google produced information, including a history of TARGET SUBJECT JOSHUA ADAM SCHULTE's Google searches (the "Google Search(es)" or "Search(es)").

21. The Google Searches, which are described in detail below, were conducted using the **Target Account** (joshschulte1@gmail.com), which the investigation has revealed belongs to SCHULTE.

22. Based on my review of those Google Searches, and conversations with law enforcement agents and others, as well as my own training and experience, I know that on or about April 4, 2016, SCHULTE conducted a Google Search that led him to visit a webpage entitled in part "Detecting USB insertion/Removal in C++ non-GUI application."⁷ I understand, based on my training, experience, and conversations with others, that "Detecting USB insertion/[r]emoval" likely relates to the function by which a computer recognizes—or does not recognize—that an external device has been connected to it via its USB port. (A USB port is a standard connection

⁶ SCHULTE retained read-only access to Project-1 (but not the ability to alter the code) and the ability to copy the computer code associated with it in order to support another project for which he had responsibility.

⁷ Both C++ and non-GUI (which stands for graphical user interface) are references to standard types of computer programming language or code, used, inter alia, by aspects of the LAN.

interface used to connect devices to a computer, including—among numerous other peripheral items—a portable computer storage device.)

23. Based on my conversations with other law enforcement agents and others, and my review of documents, I understand the following, in substance and in part:

a. On or about April 11, 2016, approximately one week later, SCHULTE unilaterally, and without authorization, logged onto the CIA Group's LAN and reinstated his own administrator privileges.

b. CIA Group management did not discover that SCHULTE had personally re-instituted his administrator privileges to the LAN without permission until on or about April 14, 2016.

24. Based on my review of the Google Searches, I know that on April 12 and 13, 2016 (*i.e.*, the time period between when SCHULTE reinstated his access to the LAN and FBI's discovery of that unauthorized reinstatement), SCHULTE conducted a series of searches apparently designed to gather information about copying a large quantity of data from one computer storage device to another, including but not limited to the following:

a. On or about April 12 and 13, 2016, in the evening,⁸ SCHULTE conducted the following Google Searches, among others:

- i. "windows command line copy all files subdirectories";
- ii. "windows copy all files and subdirectories"; and
- iii. "windows back files xcopy or robocopy"

⁸ The Google search warrant returns list the times of the searches in "UTC" or coordinated universal time, which is the same as Greenwich Mean Time. Accordingly, the dates and times of the Google Searches described herein have been adjusted to Eastern Standard Time (*i.e.*, the time zone where SCHULTE conducted the Google Searches).

I understand, based on my training, experience, and conversations with others, that “robocopy” and “xcopy” each refer to computer commands that allow a user to copy multiple computer files—or entire computer directories (and all their contents)—from one computer storage location to another. For example, this command would be used to copy files and folders, *en masse*, from one network to another, from one computer to another, or from a computer network onto a portable hard drive. According to publicly available materials published by Microsoft, the “robocopy” function would allow a user “to mirror the contents of an entire folder hierarchy across local volumes or over a network. . . . Robocopy is a powerful tool, capable of moving, copying, and deleting files and folders faster than you can say ‘Whoops.’” In addition, the Robocopy command allows a user to copy an entire file storage directory sporadically, rather than all at one time. It does that by enabling the copying process to proceed in increments and re-start from where it left off, rather than requiring a user to start the copying process over again from the beginning.

b. On the following day, April 13, 2016, SCHULTE conducted Google Searches apparently designed to gather information about the speed of various portable, external computer hard drives, such as “thumb drives” and “flash drives,” which are computer memory storage devices that connect to a computer typically via a USB port, including searches for:

- i. “thumbdrive copy speed”;
- ii. “flash drive transfer rate”; and
- iii. “flash drive read speeds”

c. Later in the day on April 13, 2016, within minutes of conducting the Google Searches regarding portable hard drive speeds, SCHULTE also conducted another Google Search apparently designed to identify the most efficient way to copy units of computer data: “optimal reading chunk size c++”. I know, based on my training, experience and conversations with other

law enforcement agents with technical expertise regarding computers, that:

i. Computers store, read and write data in units that are sometimes referred to as “blocks” or “chunks.” When data is copied, each block or chunk is separately read, copied and written from the original storage location to the destination storage location. These data blocks or chunks can be of varying sizes. Accordingly, the speed and efficiency of copying data can be affected by the size of each block or chunk of data.

ii. After conducting the above-mentioned Google Search (“optimal reading chunk size c++”), SCHULTE visited websites relating to issues such as “what is the ideal memory block size to use when copying.”

25. Based on my review of the Google Searches, I understand that on or about April 15, 2016, SCHULTE conducted the following Google Search relating specifically to software running on the CIA Group’s LAN: “[] admin view restricted pages.”⁹ After conducting the search, SCHULTE visited websites that related to ways to restrict the ability of even other Systems Administrators to view aspects of the LAN. (SCHULTE conducted the same search again thirteen days later, on or about April 28, 2016.)

26. Based on my conversations with law enforcement officers and others with knowledge of SCHULTE’s personnel file, I understand the following, in substance and in part:

a. On or about April 18, 2016, approximately four days after the CIA had learned of SCHULTE’s unauthorized reinstatement of his systems administrator privileges, SCHULTE received notice regarding CIA policies against personnel restoring their own access to privileges or computer networks after those accesses have been revoked.

⁹ The brackets redact out the proprietary name of the specific commercially available software program that was running on the CIA Group’s LAN.

b. SCHULTE signed an acknowledgment that he understood that “individuals are not permitted to personally attempt and/or renew their previous authorizations [including administrator privileges] to any particular [computer] system.” That notice further instructed SCHULTE: “do not attempt to restore or provide yourself administrative rights to any project and/or system for which they have been removed.”

27. Based on my review of the Google Searches, and my conversations with other law enforcement officers who have reviewed the Searches, I understand the following, in substance and in part:

a. Also on or about April 18, 2016 (*i.e.*, the same day he was required to sign the acknowledgement of CIA policies), SCHULTE conducted various Google Searches regarding copying files on a computer network, including “copying multiple [] large files.” After conducting this search, SCHULTE visited a website titled, in part, “how to copy a large number of files quickly between two servers.”

b. Less than a week later, on or about April 24, 2016, SCHULTE conducted a Google Search for a “SATA adapter.” Based on my training, experience and conversations with others, I understand that such an adapter is used to connect a computer hard drive to a computer externally, via USB connection. In other words, by connecting an internal drive to another computer via that computer’s external USB port, a SATA adapter allows an internal computer hard drive to be used instead as a portable, external memory drive.

c. On or about April 24, 2016, SCHULTE conducted multiple Google Searches for how to “partition” or divide a computer hard drive up, in order to move files from one storage location on the computer to a separate drive or portioned location.

d. On or about April 28, 2016, SCHULTE again conducted a Google Search

relating specifically to software running on the CIA Group's LAN: "[] admin view restricted pages," which was identical to the Search, described above, he conducted on April 15, 2016—four days after restoring his own administrator access to that very software program without authorization.

e. On the evening of Saturday, April 30, 2016, SCHULTE conducted numerous Google Searches apparently relating to the deletion of computer data, including possibly his own Google Searches, which searches included the following:

- i. "google history";
- ii. "google view browsing history";
- iii. "western digital disk wipe utility"; and
- iv. "Samsung ssd wipe utility"

I know, based on my training, experience and conversations with others, that "[W]estern [D]igital" is the name of one of the largest providers of computer storage hardware (such as portable hard drives), and that "wipe utility," or wipe drive utilities are, based on the description on Western Digital's website, designed to "erase all the data on a hard drive." I further know, based on my training, experience and conversations with others, that Samsung SSD is a reference to a brand (Samsung) of solid-state drives, which is a type of portable computer hard drive.

28. Based on my involvement in this investigation, and my conversations with other law enforcement officers involved in this investigation, I know the following, in substance and in part:

a. On March 15, 2017, the Honorable Barbara C. Moses issued a search warrant (the "March 15 Residence Search Warrant") for a Manhattan apartment located at 200 East 39th Street, Apartment 8C, New York, New York 10016, in which SCHULTE has resided

since shortly after his resignation from the CIA in November 2016 (the “Residence”).¹⁰

b. Pursuant to the search conducted on that same day, law enforcement officers recovered, among other things, numerous computer storage devices with the capacity to store at least more than ten terabytes of data, including multiple Western Digital hard disk drives (themselves totaling multiple terabytes¹¹ of storage space) and at least one Samsung SSD solid state external hard drive.¹² As noted immediately above, these are the two brands of hard drive which SCHULTE specifically searched for “wipe utilities”—programs designed to completely erase data from the drives—on the evening of April 30, 2016.¹³

29. Based on my review of the Google Searches, and my conversations with other law enforcement officers who have reviewed the Searches, I understand the following, in substance and in part:

a. At approximately 3:20 a.m. in the early morning hours of May 1, 2016 (*i.e.*, approximately five hours after conducting the Google Searches regarding the wiping of hard drives described in Paragraph 21(e) above), SCHULTE visited a website entitled in part “how can I verify

¹⁰ Previously, on March 13, 2017, Judge Moses had issued a search warrant for the same premises. The Government sought a second search warrant for an overt search of the premises because the March 13 search warrant had been executed covertly on or about March 14, 2017 and agents were not able to complete the search.

¹¹ I know, based on my training, experience and conversations with others, that one terabyte of data is roughly equivalent to one-thousand gigabytes of data or one-million megabytes of data. Put differently, one terabyte of data is roughly equivalent to more than 85 million word processing pages.

¹² Those computer devices are in the process of being analyzed.

¹³ In addition, pursuant to the search, agents recovered from SCHULTE’s apartment, internal correspondence from the CIA that appears, based on a preliminary analysis, to contain classified information (though *not* the Classified Information), including, *inter alia*, the names of CIA employees, and code names of specific CIA Group programs. I know, based on my training, experience and conversations with others, that removing and storing classified information in one’s own home is generally prohibited.

that a 1tb file transferred correctly.” I know, based on my training, experience and conversations with others, that “1tb” likely refers to 1 terabyte of data.

b. Three days later, on or about May 4, 2016, SCHULTE again conducted multiple Google Searches apparently related to the permanent deletion of data from a computer storage device, including “western digital disk wipe utility” and “can you use dban on ssd.” Based on my training, experience and conversations with others, I understand that:

i. “SSD” is an acronym for “solid-state drive” a kind of computer memory storage device.

ii. “dban” is an acronym that stands for “Darik’s Boot and Nuke,” a computer software program that is designed, according to various websites selling the software, to “securely wipe[] the hard disks of most computers. DBAN is appropriate for bulk or emergency data destruction.” According to one popular technology website, CNET.com: “use DBAN only if you want to completely eradicate any trace of data on a hard drive. This is the ultimate in data shredding—there’s no recovery once you’ve used it.”

c. Starting two days later, May 6, 2016, and again on May 8, 2016, SCHULTE conducted multiple Google Searches apparently designed to research the anonymous transmission of data on the Internet, through the use of so-called “private trackers,” which are non-public Internet sites set up to privately transfer large quantities of data from one computer to another, as well as through “The Onion Router” or “TOR,” which allows for anonymous communications on the Internet via a worldwide network of linked computer servers, and multiple layers of data encryption.

d. On May 6, 2016, SCHULTE conducted multiple Google Searches apparently relating to ways to transfer data between computers anonymously, including searches

for “trackers,” “trackers torrent,” and “private trackers.” Based on my training, experience and conversations with others, I understand that trackers or torrent trackers are computer code (or a “protocol”) that connects computers on the Internet to each other in order to facilitate the transfer of large files over the Internet. I further understand that “private trackers” are trackers that are not publicly accessible, but rather that require authorization by an administrator to use the tracker to share files. After conducting the Google Search for “private trackers,” SCHULTE visited a website entitled “opentrackers.org,” which claims that its private tracker can be used “to avoid detection & bypass anti-piracy/site blocking.”¹⁴

e. On May 8, 2016, SCHULTE conducted multiple Google Searches apparently related to the use of The Onion Router (or TOR) to anonymously transfer encrypted data on the Internet. For example, SCHULTE searched for “setup for relay,” “test bridge relay,” and “tor relay vs bridge.” Each of these searches returned information regarding the use of interconnected computers (or relays) on TOR to convey information, or the use of a computer to serve as the gateway (or bridge) into the TOR network of relays.

30. Based on my conversations with law enforcement officers and others with knowledge of SCHULTE’s personnel file and computer access, I understand the following, in substance and in part:

a. On May 26, 2016 (*i.e.*, less than three weeks after he conducted Google Searches related to the use of TOR as described above), and notwithstanding the warnings described above, SCHULTE made an official request that he again be given full access to Project-

¹⁴ Trackers and torrent trackers are often used in the transfer of large media files, including video and audio. The investigation to date has indicated that, in addition to the activity set forth in this section, SCHULTE also appears to have been engaged in the sharing of large media files, including, among other things, movies and music. Accordingly, it is at least possible that certain of these searches, as well as others described herein, could relate to those activities.

1.

b. Before receiving an official response to that request, SCHULTE requested access from another employee who, apparently without proper vetting, granted SCHULTE the requested full access to Project-1.

c. On the same day, SCHULTE used that newly obtained access to, unilaterally and without authorization, revoke the computer access permissions of all other CIA Group employees to work on Project-1.

d. Once this conduct was discovered, SCHULTE was issued a letter of warning that stated, "You were aware of the policy for access and your management's lack of support for you to retain administrative privileges, but nonetheless you took steps to deliberately violate that policy and gain those privileges." It continued by warning SCHULTE that any future violations would result in "further administrative action of a more severe nature." After receiving the letter of warning, SCHULTE disagreed with some of its conclusions and consequently refused to sign the form.

31. Based on my review of the Google Searches, and my conversations with other law enforcement officers who have reviewed the Searches, I understand the following with respect to TARGET SUBJECT JOSHUA SCHULTE's searches related to WikiLeaks, in substance and in part:

a. For the approximately six years between at least August 2010 and August 3, 2016, he conducted no searches for WikiLeaks.

b. But, beginning on August 4, 2016, SCHULTE initiated numerous Google Searches for WikiLeaks and related terms, and visited more than 200 pages that he apparently found as a result of those searches.

c. Between August 4 and August 22, 2016, SCHULTE conducted Searches for “wikileaks” at least eleven times. Pursuant to those Google Searches, he read dozens of articles regarding WikiLeaks, though he appears never to have actually visited the WikiLeaks.org Internet website.¹⁵

d. Between August 2016 and March 14, 2017, he searched “wikileaks” at least a dozen additional times, and read hundreds of online articles and publications regarding WikiLeaks. He apparently first visited the WikiLeaks.org website on March 7, 2017—the date of the release of the Classified Information.

e. In addition to the numerous searches for “wikileaks” which commenced on August 4, 2016, SCHULTE also conducted multiple related Searches, including: prior to the March 7, 2017 release of the Classified Information, “assange” (Julian Assange is the founder and “editor-in-chief” of WikiLeaks.org), “snowden its time,” “wikileaks code,” and “wikileaks 2017”—and after the March 7, 2017 release of the Classified Information, “wikileaks public opinion,” and “officials were aware before the WikiLeaks release of a loss of sensitive information.”

32. Based on my review of the Google Searches, and my conversations with other law enforcement officers who have reviewed the Searches, I further understand the following, in substance and in part:

a. On August 1, 2016, SCHULTE conducted a Google Search for “create temporary email,” and, three seconds later, visited the website www.throwawaymail.com. Based

¹⁵ I know, based on my training, experience, and conversations with others, that, among many other reasons, one reason a person might search for “wikileaks” but never visit the website is because the act of visiting a website can leave a trail that a particular IP address visited the website. Accordingly, one reason (perhaps among many) for repeatedly searching “wikileaks” but not visiting the WikiLeaks.org website, would be to avoid leaving behind a footprint of one’s visit.

on my training, experience, conversations with others, and review of documents, I know that “throwawaymail.com” is an Internet website that randomly generates an anonymous email address for a user without any registration; that random and anonymous email address can immediately receive and send emails, but automatically expires within a very short period of time (approximately 48 hours).

b. On August 10, 2016, SCHULTE conducted a Search for “tails,” and then, two seconds later, visited the website “https://tails.boum.org.” I know, based on my training, experience, conversations with others, and review of that website, that “tails” is an acronym for “the Amnesic Incognito Live System,” that works in conjunction with TOR (described above) to ensure anonymous connections on the Internet and therefore will leave no digital footprint of the internet websites visited by someone using the system.¹⁶ The WikiLeaks.org website also lists “tails” as one of its “partner organizations.”

c. On August 14, 2016, SCHULTE searched various topics regarding employment litigation and disputes, including filing a lawsuit against one’s boss (*e.g.* “can you sue your boss”), one’s employer (*e.g.* can i sue my employer for unfair treatment”), and the “EEOC.” (Less than an hour after conducting those Searches, SCHULTE searched “tor.”)

d. On September 1 and 5, 2016, SCHULTE repeatedly searched, “what is a mole.” I know, based on my training and experience that, among other meanings, a “mole”

¹⁶ News reporting indicates that Edward Snowden used the tails system in connection with his transfer of allegedly classified documents to various news outlets. *See Out in the Open: Inside the Operating System Edward Snowden Used to Evade the NSA*, Wired, April 14, 2014, *available at* <https://www.wired.com/2014/04/tails/> (last accessed Mar. 31, 2017); The ultra-secure Tails OS beloved by Edward Snowden gets a major upgrade, PC World, Jan. 27, 2016, *available at* <http://www.pcworld.com/article/3026721/linux/the-ultra-secure-os-beloved-by-edward-snowden-gets-a-major-upgrade.html> (last accessed Mar. 31, 2017).

generally refers to a spy working inside a country's security, military or intelligence services.

33. Based on my conversations with law enforcement officers and others familiar with TARGET SUBJECT JOSHUA SCHULTE's employment history with the CIA, including his security clearances and related investigations, I understand the following, in substance and in part:

a. In approximately August 2016, as part of a standard background reinvestigation of SCHULTE for the purpose of renewing his security clearances, the CIA conducted interviews of multiple CIA Group colleagues. Among other things:

b. Some (but not all) colleagues independently reported that SCHULTE's demeanor with his management and colleagues, and his commitment to his work, changed markedly for the worse in or around February 2016.

c. Multiple colleagues stated that SCHULTE had indicated that he felt aggrieved by the CIA in a number of respects. Some also reported that they believed SCHULTE to be untrustworthy and potentially subject to outside coercion. (Other colleagues made no such report and, indeed affirmatively reported that they believed that SCHULTE was, in fact, trustworthy.)

d. Some (but not all) colleagues also reported that SCHULTE's security practices were lax, and that SCHULTE tended not to abide by security guidelines he deemed inconvenient—particularly guidelines concerning when and what kinds of media or data (such as external drives) could be connected or uploaded to CIA computer systems.¹⁷

34. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know in substance and in part that, in

¹⁷ As described herein, external drives can be connected to computers and files in order to allow users to move files from the computers onto the portable external drives.

connection with and preceding SCHULTE's November 2016 resignation from the CIA:

a. Approximately one month prior to his resignation, on October 12, 2016, SCHULTE, using his CIA email account, sent an email to another CIA Group employee at that employee's official email account. The subject line of the email stated, "ROUGH DRAFT of Resignation Letter *EYES ONLY*." The email contained a letter entitled "Letter of Resignation 10/12/16" and addressed to "To whomever it may concern" ("Draft Resignation Letter"). I know from reviewing the Draft Resignation Letter, which spanned approximately three single-spaced pages, the following:

i. SCHULTE began the letter by stating, in substance and in part, that he had "always been a patriot" and would "obviously continue to support and defend this country until the day that I die," but that "from this day forward" he would "no longer do so as a public servant."

ii. SCHULTE claimed that he believed that the CIA Group management had unfairly "veiled" CIA leadership from various of SCHULTE's previously expressed concerns, including concerns about the network security of the CIA Group's LAN. SCHULTE continued: "That ends now. From this moment forward you can no longer claim ignorance; you can no longer pretend that you were not involved."

iii. SCHULTE explained that he was resigning from the CIA because CIA Group management had, among other things, "ignored" issues he had raised about "security concerns" and had attempted to "conceal these practices from senior leadership," including that the CIA Group's LAN was "incredibly vulnerable" to the theft of sensitive data. He claimed that one named CIA Group manager had ignored his security concerns and "later attempt[ed] to evade responsibility and blame the decentralized and insecure [CIA Group computing] environment

entirely on me.”¹⁸

iv. Specifically, SCHULTE wrote that inadequate CIA security measures had “left [the CIA Group’s LAN] open and easy for anyone to gain access and easily download [from the LAN] and upload [sensitive CIA Group computer code] in its entirety to the [public] internet.”

b. It appears that SCHULTE did not, in fact, submit the Draft Resignation Letter to the CIA.

c. On his last day with the CIA (November 10, 2016), SCHULTE did, however, send an internal email to the CIA Office of the Inspector General (OIG) advising that he had been in contact with the United States House of Representatives’ Permanent Select Committee on Intelligence regarding his complaints about the CIA (the “OIG Email”).

i. In the OIG Email, which SCHULTE labeled “Unclassified,” SCHULTE raised many of the same complaints included in the draft “Letter of Resignation 10/12/16,” described above, including the CIA’s treatment of him and its failure to address the “security concerns” he had repeatedly raised in the past.

ii. Shortly thereafter, CIA security learned that one of SCHULTE’s colleagues had witnessed SCHULTE printing the OIG Email, placing it in a folder, and exiting the CIA Component facility where SCHULTE worked. Notwithstanding SCHULTE’s labeling of the email as “Unclassified,” the CIA subsequently determined that the OIG Email, which SCHULTE removed from the CIA without authorization, did in fact contain classified information.

¹⁸ SCHULTE went on to describe other complaints he had about managers at the CIA. Among other things, SCHULTE described his complaints about the way in which CIA Group management had handled various personnel and disciplinary issues.

35. Based on my involvement in this investigation, and my conversations with other law enforcement officers involved in this investigation and/or my review of reports prepared in the course of this investigation, I understand that the FBI recovered a copy of the November 10, 2016 OIG Email, which contained classified information and which SCHULTE labeled “Unclassified” and removed from a CIA facility, from his residence during the March 15, 2017 search.

36. Based on my conversations with other law enforcement agents and others, and my review of documents, I also understand that, following the March 7, 2017 publication of the Classified Information on WikiLeaks, SCHULTE repeatedly initiated contact, via telephone and text messages, with multiple of his former CIA Group colleagues. Those colleagues reported that contact to government and law enforcement officials. In particular, I know the following regarding SCHULTE’s communications in the days following March 7, 2017:

- a. In those communications with his former colleagues, SCHULTE repeatedly asked about the status of the investigation into the disclosure of the Classified Information.
- b. SCHULTE requested more details on the information that was disclosed.
- c. SCHULTE inquired of his interlocutors’ personal opinions regarding who, within the CIA Group, each believes is responsible for the disclosure of the Classified Information. SCHULTE also asked what other former CIA Group colleagues are saying about the disclosure.
- d. SCHULTE repeatedly denied any involvement in the disclosure of the Classified Information.
- e. SCHULTE indicated the he believes that he is a suspect in the investigation of the leak of Classified Information.

37. Furthermore, I have learned that SCHULTE specifically used the **Target Account**, *i.e.*, the account associated with the Gmail account joshshulte1@gmail.com, to make some of the inquiries described above. For example:

a. I know from records previously obtained from Google that, on or about March 7, 2017, when WikiLeaks released the Classified Information, SCHULTE used the Google Voice feature associated with the **Target Account** to send approximately 149 texts to multiple of his former colleagues at the CIA.

b. I have learned from other FBI agents who have spoken with some of SCHULTE's former colleagues at the CIA that SCHULTE, using the Google Voice feature associated with the **Target Account**, also had phone calls with former CIA colleagues, including one telephone call with a former colleague in which he, among other things, inquired of the former colleague's personal opinions regarding who was responsible for the disclosure of the Classified Information and what the person's motivation might be. SCHULTE indicated on this call that he believed that the person responsible was a contractor who disclosed the Classified Information for fame.

c. I have further learned from other FBI agents who have spoken with some of SCHULTE's former colleagues at the CIA that, in a call using the telephone number associated with the **Target Account** on or about March 8, 2017 with the same former colleague, SCHULTE denied his involvement in the disclosure of the Classified Information, indicated his belief that many people suspected him of the disclosure, and relayed a conversation with another acquaintance in which SCHULTE had denied involvement in the disclosure of the Classified Information, but was dissatisfied with the acquaintance's reaction to SCHULTE's denial.

B. Probable Cause Relating to CP Offenses

38. As described above, On March 15, 2017, the Honorable Barbara C. Moses issued a search warrant authorizing a search of SCHULTE's residence in Manhattan—the March 15 Residence Search Warrant. Based on my involvement in this investigation, and my conversations with other law enforcement officers involved in this investigation as well as my review of documents prepared in the course of this investigation, I understand the following, in substance and in part:

a. During the execution of the March 15 Search Warrant, law enforcement officers recovered, among other things, multiple computers, servers, and other portable electronic storage devices (the “Schulte Devices”). Following the seizure of the Schulte Devices, the devices were transported by the FBI for analysis and examination to a U.S. Government facility in Herndon, Virginia, within the Eastern District of Virginia.

b. In the course of searching the Schulte Devices for evidence, fruits, and instrumentalities of the National Security and Computer Crime Offenses, agents discovered a photograph on SCHULTE's desktop computer that appeared to depict child pornography (the “CP Picture”). An agent who is assigned to the Crimes Against Children Squad (the “CACS Agent”) reviewed the CP Picture and believed that the CP Picture depicted a naked young child on all fours and what appear to be two adults around her, one of whom appears to be performing a sexual act on the child—oral sex around the child's buttocks. The CACS Agent also believed that the child was a minor based on, among other things, body structure, lack of breast development, and lack of pubic hair.¹⁹

¹⁹ Based on my conversations with the CACS Agent, I understand that it is possible that the CP Picture (like many photographs of child pornography) could be altered and not a real picture. However, the CACS Agent had only reviewed a printout of the CP Picture. Members of the FBI who analyzed the Desktop Computer have informed me that the CP Picture looks more

c. Following the discovery of the CP Picture, search warrants were issued in the Eastern District of Virginia that expanded the scope of the search of the Schulte Devices to include evidence, fruits, and instrumentalities of the CP Offenses, as well as Copyright Offenses. Although the search of the Schulte Devices is ongoing, agents have encountered on one of the Schulte Devices a volume of files (the "Volume"), approximately 54 GB in size, that contains several layers of encryption. Agents have been able to access the encrypted Volume, which contains what appeared to be hundreds of files organized into separate folders. Some of the folders are labeled "downloads," "kids," "old," "other," and "young."²⁰

d. One of the files in the Volume is a video with the filename "pthc maryann 2yo suck.mpg." The video depicts a prepubescent girl, estimated to be younger than five years old, with her mouth on an adult's penis. Another file in the Volume, with the filename "real underage fuck cum baby 2yo rape.mpg," is a video that contains multiple scenes. The first scene depicts what appears to be an adult male placing his finger, and later his penis, inside the vagina of a prepubescent girl, estimated to be younger than five years old.

C. Probable Cause for Evidence of Copyright Offenses

39. Based on my conversations with members of the FBI who were involved in searching the Schulte Devices for evidence, fruits, and instrumentalities of the National Security and Computer Crime Offenses pursuant to prior search warrants, I have learned, among other things, that at least one of the servers recovered from SCHULTE's Manhattan residence ("Server-1") has indications that SCHULTE was involved in illegally sharing copyrighted movies over the

like an actual photo when viewed on the computer as opposed to when printed. I know that an agent involved in this investigation has viewed the CP Picture on the Desktop Computer and concluded that it is an actual photograph.

²⁰ The search warrants in the Eastern District of Virginia were issued on or about April 14, 2017 and May 10, 2017.

Internet. Specifically, Server-1's command log (which shows the history of commands sent to Server-1 by the user, likely via a computer connected to Server-1), indicates that SCHULTE participated in the sharing of dozens of movies using torrent trackers.²¹ As described above, based on my training, experience and conversations with others, I understand that torrent trackers are computer protocol which connect computers on the Internet to each other in order to facilitate the transfer of large files over the Internet.

40. Based on my training, experience, and my conversations with another FBI agent who has reviewed the public catalog of copyrighted works available through the United States Copyright Office, I know that most, if not all, of the movies that SCHULTE appears to have participated in sharing are copyrighted works registered with the United States Copyright Office. For example, among the many movies that were apparently shared include *Hacksaw Ridge*; *The Revenant*; *Captain America: Civil War*; and *The Hateful Eight*, all of which are copyrighted works currently registered with the United States Copyright Office.

41. Based on my involvement in this investigation as well as my review of reports prepared in the course of this investigation, I understand that in or about March 2017, FBI agents conducted interviews of multiple CIA employees who know SCHULTE, and that, among other things, one of those employees stated that SCHULTE operates a service allowing users to stream movies over the internet (the "Streaming Service") and that SCHULTE manages the accounts of users of the Streaming Service.

²¹ Upon viewing the command log, which was searched pursuant to a prior search warrant for evidence regarding the National Security and Computer Crime Offenses, and upon seeing indications of illegal movie sharing, members of the FBI stopped viewing the command log and contacted the U.S. Attorney's Office. A warrant was then obtained to search for evidence, fruits, and instrumentalities of the Copyright Offenses.

42. Based on my review of a telephone that was among the Schulte Devices searched for evidence, fruits, and instrumentalities of the National Security and Computer Crimes Offenses pursuant to the terms of the March 15 Residence Search Warrant, I have learned, among other things, that on or about October 31, 2016, SCHULTE, using a Gmail address associated with the **Target Account**, sent an email to approximately 20 other individuals with the subject line “Pedbsktbll Plex Server Downtime 11/9/2016-1/2017” (the “Email”). In the Email, SCHULTE notifies the recipients that the “server will be down as it relocates to NYC starting 11/9. Thus, you will have the next 9 days to select and download material you may wish to watch during that downtime. Hopefully, the server will be back and running mid to late December – January at the latest.” Based on my training, experience, and participation in this investigation, I believe that SCHULTE was referring to the Streaming Service and was alerting users that the service would be unavailable while he moved to New York in late 2016.

* * *

43. I respectfully submit that there is probable cause therefore to believe that the **Target Account** contains evidence, fruits, and instrumentalities of the Subject Offenses. Among other things, I respectfully submit that there is probable cause to establish that SCHULTE is proficient in and makes use of Internet-based computing services, including those offered by the Provider through the **Target Account**.

44. Moreover, based on my training and experience, I know that individuals who engage in the Subject Offenses often use Internet-based services (like the **Target Account**) as a means by which to communicate with co-conspirators as well as means through which not only to transmit but also to store purloined information so that they do not have to carry it on their person. In addition, I know that individuals who engage in the Subject Offenses use Internet-based services

like the **Target Account**, to conduct searches that are relevant to committing or to avoiding detection for crimes such as the Subject Offenses.

45. Finally, I know that individuals who engage in the Subject Offenses oftentimes use Internet-based computing services, like the **Target Account**, to publish purloined information. For example, based on my training and experience and my involvement in this investigation, I know that WikiLeaks is an Internet-based publication and that individuals who provide information to WikiLeaks in the past oftentimes have done so through the use of other Internet-based computing platforms, like the **Target Account** and other services offered by the Providers. Accordingly, when each of these factors is considered in conjunction with the fact of SCHULTE's access to the purloined information, his clear proficiency in computers and computer-programming, his extensive prior use of the **Target Account** related to the commission of the Subject Offenses, and the probable cause establishing SCHULTE's access to and use of the **Target Account**, I respectfully submit that there is probable cause to believe that the **Target Account** will contain evidence, fruits, and instrumentalities of the Subject Offenses.

46. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for service of a search warrant issued under § 2703, or for the collection or production of responsive records. Accordingly, the warrants requested herein will be transmitted to the Providers, which will be directed to produce a digital copy of any responsive records to law enforcement personnel within 10 days from the date of service. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will retain the records and review them for evidence,

fruits, and instrumentalities of the Subject Offenses as specified in Section III of Attachment A to the requested warrants, which shall not be transmitted to the Providers.

47. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all content associated with the **Target Account**. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, to the extent applicable, including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.


VI. Request for Non-Disclosure and Sealing Order

48. The existence and scope of this ongoing criminal investigation are not publicly known. As a result, premature public disclosure of this Affidavit or the requested warrants could alert potential criminal targets that they are under investigation, causing them to destroy evidence, flee from prosecution, or otherwise seriously jeopardize the investigation. In particular, given that targets of the investigation are known to use computers and electronic communications in

furtherance of their activity, the targets could easily delete, encrypt, or otherwise conceal such digital evidence from law enforcement were they to learn of the Government's investigation.

49. Accordingly, there is reason to believe that, were the Provider to notify the subscriber(s) or others of the existence of the requested warrants, the investigation would be seriously jeopardized. Pursuant to 18 U.S.C. § 2705(b), I therefore respectfully request that the Court direct the Provider not to notify any person of the existence of the warrant for a period of 180 days from issuance, subject to extension upon application to the Court, if necessary.

50. For similar reasons, I respectfully request that this Affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and Affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.



JEFF D. DONALDSON
Special Agent
Federal Bureau of Investigation

Sworn to before me on
this 17th day of May 2017.



S/Gabriel W. Gorenstein

THE HONORABLE GABRIEL W. GORENSTEIN
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All
Content and Other Information for the
Google account associated with Email
Address joshschulte1@gmail.com,
Maintained at Premises Controlled by
Google, Inc. and Google Payment
Corp.

17 MAG 3734

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Google, Inc. and Google Payment Corp. (collectively "Google")

The Federal Bureau of Investigation (the "FBI" or the "Investigative Agency")

1. Warrant. Upon an affidavit of Special Agent Jeff D. Donaldson of the FBI and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds that there is probable cause to believe that content information maintained at premises controlled by Google associated with the email address joshschulte1@gmail.com contains evidence, fruits, and instrumentalities of a crime, all as specified in Attachment A hereto. Accordingly, Google is hereby directed to provide to the Investigative Agency, within 10 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A, which shall not be transmitted to the Provider. The Government is required to serve a copy of this Warrant and Order on Google within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which Google is capable of accepting service.

2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, danger to the physical safety of an individual, flight from prosecution, and/or intimidation of potential witnesses or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that Google shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of 180 days from the date of this Order, subject to extension upon application to the Court if necessary, except that Google may disclose this Warrant and Order to an attorney for Google for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on Google; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

May 17, 2017
Date Issued

3:42 PM
Time Issued

S/Gabriel W. Gorenstein
THE HONORABLE GABRIEL W. GORENSTEIN
United States Magistrate Judge
Southern District of New York

Attachment A

I. The Target Account and Execution of Warrant

This warrant is directed to Google, Inc. and Google Payment Corp. (collectively, “Google” or the “Provider”) and applies to all content and other information within Google’s possession, custody, or control that is associated with the email address joshschulte1@gmail.com (the “**Target Account**”).

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to Google. Google is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below, a copy of which shall not be transmitted to the Provider.

II. Information to be Produced by Google

To the extent it is within Google’s possession, custody, or control, Google is directed to produce the following information associated with the **Target Account**:

a. Search History. All data concerning searches run by the user of the **Target Account**, including, but not limited to, the content, date, and time of the search.

b. Google+ Photos and Content. All data concerning Google+ Photos, including all albums, photos, videos, and associated metadata for each file, as well as all Google+ posts, comments, profiles, contacts, and information relating to Google+ Circles.

c. Google Drive Content. All files and folders in the Google Drive associated with the **Target Account**.

d. Google Voice. All records, voicemails, text messages, and other data associated with Google Voice.

e. *Google Wallet Content.* All data and information in the Google Wallet associated with the **Target Account**.

f. *YouTube Content.* For any YouTube account associated with the **Target Account**, all subscriber information as well as copies of any videos and associated metadata and any YouTube comments or private messages.

g. *Android Content.* Any Android device information associated with the **Target Account**, including IMEI/MEID, make and model, serial number, date and IP of last access to Google, and a list of all accounts that have ever been active on the device.

h. *Email Content.* All emails sent to or from, stored in draft form in, or otherwise associated with the **Target Account**, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email).

i. *Address book information.* All address book, contact list, or similar information associated with the **Target Account**.

j. *Subscriber and payment information.* All subscriber and payment information regarding the **Target Account**, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

k. *Linked accounts.* The account identifiers for all accounts linked to the **Target Account**, and subscriber records therefore as described in the preceding sub-paragraph, including but not limited to any account linked to the **Target Account** by registration IP address, “machine” or other cookie, alternate email address, or telephone number.

l. Transactional records. All transactional records associated with the **Target Account**, including any IP logs or other records of session times and durations.

m. Customer correspondence. All correspondence with the subscriber or others associated with the **Target Account**, including complaints, inquiries, or other contacts with support services and records of actions taken.

n. Advertising ID and DoubleClick records. The Advertising IDs assigned to devices associated with the **Target Account**, and all DoubleClick or other records of internet activity associated those Advertising IDs.

o. Preserved records. Any preserved copies of any of the foregoing categories of records created in response to any preservation request(s) issued pursuant to 18 U.S.C. § 2703(f).

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by Google in order to locate:

(i) any evidence, fruits, and instrumentalities of the unauthorized possession and, *inter alia*, the communication of national defense information to someone not entitled to receive it, in violation of Title 18, United States Code, Section 793(d); the unlawful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); exceeding authorized access to a computer in order to obtain national defense information with reason to believe that information could be used to the injury of the United States and the advantage of a foreign nation and willfully transmitting that information to a person not entitled to receive it, in violation of Title 18, United States Code, Section 1030(a)(1); intentionally exceeding authorized access to a computer and thereby obtaining information from a department or agency of the United States, in violation of Title 18, United States Code, Section 1030(a)(2)(B) (the “National Security and Computer Crime Offenses”), for the time period March 14, 2017 to the present; and

(ii) any evidence, fruits, and instrumentalities of (i) violations of Title 18, United States Code, Section 2252 (possession, transportation, receipt, distribution, production, and reproduction of sexually explicit material relating to children) and Title 18, United States Code, Section 2252A (activities relating to material constituting or containing child pornography) (the “CP Offenses”); and (ii) violations of Title 17, United States Code, Section 506 and Title 18, United States Code, Section 2319 (criminal infringement of a copyright) (the “Copyright Offenses”) (collectively, with the National Security and Computer Crime Offenses and the CP Offenses, the “Subject Offenses”), for the time period May 17, 2007 through the present.

Such evidence, fruits, and instrumentalities of the Subject Offenses include the following:

- a. Evidence of the identity(s) of the user(s) of the **Target Account** as well as other coconspirators in contact with the **Target Account**;
- b. Evidence relating to the geolocation and travel of the user(s) of the **Target Account** at times relevant to the Subject Offenses;
- c. Evidence relating to the participation in the Subject Offenses by the users of the **Target Account** and others;
- d. Evidence concerning financial institutions and transactions used by the users of the **Target Account** in furtherance of the Subject Offenses;
- e. Communications evidencing crimes, including but not limited to correspondence with others relating to the Subject Offenses;
- f. Evidence of and relating to computers or other online accounts and facilities (such as additional email addresses) controlled or maintained by the user of the **Target Account**; and
- g. Passwords or other information needed to access any such computers, accounts, or facilities.